PUBLIC ACCOUNTS AND ESTIMATES COMMITTEE

TWENTY-SIXTH REPORT TO PARLIAMENT

INFORMATION TECHNOLOGY AND THE YEAR 2000 PROBLEM - IS THE VICTORIAN PUBLIC SECTOR READY?

NOVEMBER 1998

Ordered to be printed

VICTORIAN GOVERNMENT PRINTER
1998

No. 24 Session 1998

Table of Contents

CHAPTER 8 : THE LEGAL IMPLICATIONS OF THE YEAR 2000 PROBLEM

CHAPTER 9 : COMMUNITY ASSURANCES

APPENDICES

Public Accounts and Estimates Committee

Members

Hon. W Forwood, MLC (Chairman)
Mr S P Bracks, MP (Deputy Chairman)
Hon. R Best, MLC
Mr R J Hulls, MP
Mr P J Loney, MP[(i)]
Hon. N B Lucas, MLC
Mr S J McArthur, MP
Hon. T C Theophanous, MLC
Mr K A Wells, MP

The Committee's address is :

Level 8
35 Spring Street
Melbourne Victoria 3000

Telephone enquiries: (03) 9651 3556

Facsimile: (03) 9651 3552

Email: paec@parliament.vic.gov.au

Internet: htpp://www.parliament.vic.gov.au/paec/default.htm

(i) Appointed 3 September 1998

Membership of the Sub-Committee

Members

This Inquiry was undertaken by:

Mr S J McArthur, MP (Chairman of this Inquiry)
Hon. W Forwood, MLC
Mr R J Hulls, MP
Hon. T C Theophanous, MLC

For this Inquiry, the Sub-Committee was supported by a secretariat comprising:

Ms M Cornwell, Executive Officer
Mr J Arnol, Research Officer, seconded from the Victorian Auditor-General's Office
Ms F Essaber, Office Manager

Specialist Advisors to the Sub-Committee:

Technical advisor:

Professor B. J. Garner, School of Computing & Mathematics, Deakin University

Legal advisor:
Ms. M. de Zwart, Faculty of Law, Monash University

Duties of the Committee

The Public Accounts and Estimates Committee is a joint parliamentary committee constituted under the *Parliamentary Committees Act* 1968, as amended.

The Committee comprises nine Members of Parliament drawn from both Houses of Parliament and all parties.

The Committee carries out investigations and reports to Parliament on matters associated with State financial management. Its functions under the Act are to inquire into, consider and report to the Parliament on:

a) any proposal, matter or thing connected with public administration or public sector finances;
b) the annual estimates or receipts and payments and other budget papers and supplementary estimates of receipts and payments presented to the Assembly and the Council;

if the Committee is required or permitted so to do by or under the Act.

As a result of recent changes to the Audit Act the Committee, in consultation with the Auditor-General, determines the objectives of performance audits and identifies any particular issues that need to be addressed during these audits.

Glossary

Apple MacIntosh PCs	The hardware, operating system and applications that run on Apple MacIntosh computers are Year 2000 compliant until 2040.
Applications	Also referred to as business solutions, are software programs that instruct the computer to perform a particular task such as accounting, payroll, word processing, publishing, project management or to operate computer hardware. Applications which bypass the OS and BIOS to obtain data directly from the RTC may receive incorrect dates.
ASX	Australian Security Exchange.
Backup	A copy of the data held in computer files for use in the restoration of the database after computer failures/crashes.
BIOS	The Basic Input/Output System is a ROM chip that holds basic start-up information for the computer. For example it tells the CPU where the keyboard is, the types of disk drives it has, which drive to boot from etc. The BIOS retrieves the date and time from the RTC and feeds it to the OS and applications. Most BIOS chips use four digit years but only ever change the last two digits and most newer BIOS setups will automatically correct “00” to “2000”. Some OS will also correct the problem automatically.
Bug	A computer programming error. To eliminate or fix a bug requires the reprogramming of computer code and reiterative testing of the new program.
Business continuity	The continuation of normal business operations and service delivery in the event of disruptions such as power outages, gas shortages or the malfunction of business critical computer systems. Business continuity is the main purpose for developing contingency plans.

Business critical	Information technology-based systems (software, hardware and data communication links, including embedded chip technology, such as monitoring, dispensing and telemetry systems) whose sudden, temporary or permanent unavailability or unreliability would compromise the quality, quantity or timing of their service delivery and includes systems associated with: • health and safety; • community security; • emergency services; • utility services; and • revenue collection and distribution. See also 'mission critical'.
Century date rollover	The cusp of 1999 and 2000 when the "99" becomes "00". As a precaution even compliant computers should be turned off on 31 December 1999 and started again the next day to allow the computer to reset the date to 2000.
Certification	The process used by independent auditors to verify the Year 2000 compliance status of computer systems.
Chips	Silicon based semi-conductors or microprocessors, which contain thousands of transistors designed to respond to digital binary data to produce results to complex computations.
Client-server network	A network of computers connected via server computers. Files held on servers are accessed and data is transferred to client applications.
COBOL	Common Business Orientated Language. An early programming language now in demand for fixing the Year 2000 problem, as are skills in CICS, DB2 and PL/1.
Compliance	There is no single accepted definition of Year 2000 compliance, which has led to a number of terms such as 'Year 2000 ready' or 'Year 2000 capable'. The ASX has adopted the British Standards Institutions Year 2000 Compliance Rules described in DISC PD2000-1. The British standard has been adapted to form Australian Standards eg. the Australian/New Zealand HB 120-1998 Year 2000 Compliance Standard for small to medium enterprises.

Contingency plan	A plan of actions that will ensure the continuation of business operations eg. the creation of manual over-rides for automated processes, the use of stockpiled parts for JIT systems or the use of alternative energy supplies to electricity and natural gas.
Conversion	The modification or addition of computer source code to change non-compliant systems into Year 2000 compliant systems.
CPU	Central processing unit. The main computational microprocessor of a computer rated according to its transistor capacity to speed.
Date arithmetic	Mathematical calculations that include date/time data. For example, most forecasting models for investment returns, superannuation payments, interest and dividends use date arithmetic. Also used in embedded systems to automate security and warning devices, the flow of medication in biomedical equipment etc.
Date-dependent	Or ‘date-sensitive’. Computer hardware, embedded chips and software applications that require date data to execute their tasks. Non-compliant two-digit dates will create problems such as inaccurate answers or the malfunction of devices.
Desktop system	A stand alone computer that has its own CPU and storage. The PC can be connected to a network as an intelligent work station and will function independently if disconnected from the network.
Disaster Recovery Plan	A plan that analyses and deals with the risks faced by a business to permit business continuity and the recovery of data and computer functionality in the event of disasters such as the total loss of power supplies e.g. offsite back-up, UPS systems.
DOS	Disk operating systems store operating system software on the internal hard drive or disk of a computer.
EDI	Electronic data interchange allows commercial transactions to take place via computers between trading partners. Data that includes date fields will need to be tested at each transfer to prevent non-compliant data entry

Embedded System	Independent computer chips that operate a wide variety of non-computer machines, electronic devices and systems, such as plant control systems, biomedical equipment, electric appliances, communication and navigation equipment. See Appendix 8 for a list of embedded technology systems.
Firewall	Software in an area of a computer or more commonly in a separate computer system, which filters incoming and outgoing content to prevent unauthorised access to the main computer system or, in the case of Year 2000 problem, prohibits the transfer of non-compliant data.
GIS	Geographic information systems allow the linking of data to geographic locations on a computer-based map.
GPS	Global positioning satellite system.
Hardware	The visible components of the computer such as the CPU, motherboard, memory modules - as opposed to the unseen software or codes that pass through the hardware.
HVAC	Heating/ventilation/air-conditioning system. An automated environmental control system. Without HVACs rooms containing electronic sensors and heat-sensitive data processing equipment can overheat and malfunction.
IBM/compatible PCs	Computers that have the same design features of the IBM PC. The first Year 2000 compliant IBM PCs (and servers) were introduced after 1 January 1996. Some earlier models may be manually reset by typing "Date 01/01/2000" at the DOS prompt[1] – see *www.cnet.com/Content/Reports/Special/Y2K/*.
Interface	Date data fields that are transferred between computers in different organisations are made through a computer interface. Interfaces usually refer to lists of all the electronic links between software. For example, a link to the bank to process EFTs.

[1] Warning: Some Year 2000 test programs may cause applications to malfunction, lose data or software licences to expire. Close date-sensitive programs, make backups of any crucial data and applications before running tests.

Internet	A global computer network that allows users to access and share information held in computers on world wide websites. All web sites have links with other sites that share common topics and information.
Inventory	A detailed list of functions and items that may be affected by the Year 2000 problem categorised by business component and including all software, hardware, office equipment (eg photocopiers), building functions (eg lights), supply chains and external suppliers (eg. electricity, stationers, etc).
IT	Information technology, such as the technology that permits the storage, retrieval and processing of digital information.
JIT	A just in time system uses a computer-controlled inventory, ordering and delivery system for the manufacture or production of goods. JIT for instance is used to re-stock supermarket shelves, to order parts for assembly lines etc.
Leap year	2000 is a leap year. Although some programmers knew that every fourth year was a leap year, an exception occurs for centuries – only every fourth century is a leap year.
Legacy systems	Software applications that were created in-house in the 1960s and 70s for specific business solutions such as taxation systems, licensing and registration systems, payroll, financial management etc. Due to past programming practice all are affected by the Year 2000 problem.
Mainframe	A large computer system for managing very large databases, network and systems management, and computer-intensive applications. These systems usually run legacy applications.
Masking	Or date encapsulation. The favoured solution over date expansion or windowing techniques due to lower cost and faster implementation. The technique involves date-shifting code or data by 28, thus all date data is correct in terms of the days of the month but false in terms of the year.

Microprocessor	A silicon chip that incorporates thousands of transistor switches that individually and systematically respond to binary codes to compute results.
Mid-range	Large computers that are smaller than mainframes but larger than PCs.
Millennium Bug	A computer “bug” which will cause malfunctions at the beginning of the third millennium due to the inability of most computer applications and hardware, including date dependent embedded systems, to recognise the year “2000”.
Mission Critical	Applications, computer systems or embedded devices that will prevent the continuation of core business functions if they are taken out of service. For example, the financial management systems in a bank or PLCs in plant control systems. See also ‘business critical’.
Motherboard	Comprises all of the chipsets in the computer including the CPU, RTC, BIOS, and other chipsets on a single circuit board to which all of a computer’s peripheral hardware is connected.
Non-compliant	A computer system, software application or embedded chip that cannot correctly process the date “2000”. When tested such systems fail Australian compliance standards, which require continued functioning before, on and after 1 January 2000.
OS	Operating system, also referred to as platforms. An essential program that tells the CPU how to control both hardware and application software. Examples include DOS, UNIX, OS/2, Windows 95 and Windows NT. The BIOS supplies the date to the OS and thereon to other programs. Some OS read dates directly from the RTC and will create Year 2000 problems for date sensitive applications.
Patches	Lines of computer source code that will fix or eliminate known computer programming errors. Patches can introduce new problems such as reducing CPU performance or create unstable operating environments. Patches to repair the Year 2000 problem in the BIOS, OS or applications can be downloaded from the Internet.

PC	Personal computer. Most 486 or earlier PCs, many of the early Pentium PCs 60/75/90 etc. are affected by the Year 2000 problem. It is estimated that only 2 per cent of the world's 300 to 400 million PCs have been checked for 2000 compliance.[2]
PLCs	Programmable logic controllers is the technically correct term for embedded systems. PLCs occur in electricity generation plant controls, airconditioning systems, automated doors, food production lines, lift services, traffic control signals and remote control systems.
Remediation	The process of repairing the Year 2000 problem in computers or devices containing affected embedded chips, either through modification, replacement or retirement.
ROM	Read only memory.
RTC	Real time clock. A clock counter that uses a back-up battery when the computer is off. Standard RTCs can only store the last two digits of the year. The clock is read by the BIOS and the BIOS passes the date on to other programs. In some cases software applications bypass the BIOS to get the time and date directly from the RTC.
RTU	Remote telemetry unit. Devices that monitor physical conditions and send data eg. currents, pressure, temperature, volume etc. to a central control system.
SCADA	Supervisory Control and Data Acquisition systems are plant control systems that receive data from remote sensors or telemetry devices to control valves, shut-off mechanisms etc.
SMEs	Small to medium-sized enterprises. These businesses represent 58 per cent of Australia's GDP and employ 3.6 million people. Up to 40 per cent of SMEs have taken no action to prevent the Year 2000 problem from occurring in 2000[3]. Victoria has 55,000 SMEs.

[2] Greenwich Mean Time Consultants, London, reported in *The Australian* 6 October 1998, p.30 and *The Age*, 6 October 1998, p.5.
[3] Hon. Mark Birrell, Minister for Industry, Science and Technology, *Herald Sun* 27 September 1998, p.61

Software	The invisible binary codes which are programmed so that computers can perform particular tasks and calculations. Most software created throughout the 60s, 70s, and 80s will be affected by the Year 2000 problem as will much of the software created in the 90s.
Spreadsheet	An end user developed application, which organises data into rows and columns and allows calculations to be performed in the resulting data cells. Date data contained in spreadsheet cells can be corrupted by the Year 2000 problem.
UPS	Uninterruptible power supply. The UPS safeguards against surges, spikes and electrical noise and can power the average PC for more than 10 minutes in the event of power loss.
Whole of Government	A holistic view of all government operations.
Y2K	Year 2000 - “K” is for kilo, the Greek word for thousand.

Chairman's Introduction

One function of the Public Accounts and Estimates Committee is to follow up issues raised by the Auditor-General. This Inquiry is one such case, and was chosen because the Committee believed that the Year 2000 Problem was not well understood, and is of vital importance.

Both these concerns have been addressed in this Report.

It is appropriate that the Committee report now, as time for coping with the problem is disappearing fast.

At the outset, it is crucial to state the Committee's view that the Year 2000 problem is not a doomsday scenario, and it specifically rejects that prospect. Indeed, it may well be that worse problems will be caused because of fear of what might happen, than by what actually occurs.

In fact, what will happen is uncertain. What is certain is that there will be unexpected events. The challenge to us all is to limit the unexpected by diligent preparation and remediation work, and to prepare contingency plans. Again, I trust that this Report will assist in meeting the challenge.

This is not so much a computer issue as a risk management one.

The Inquiry was undertaken by a Sub-Committee, chaired by Steve McArthur and including Theo Theophanous, Rob Hulls and myself. I thank my colleagues for their dedicated efforts to a complex task.

The Committee would also like to thank the many officials who responded to its survey or provided input through the *in camera* hearings.

The Committee benefited from the technical advice provided by Professor Brian Garner and the legal advice from Ms Melissa de Zwart. They contributed immeasurably to our understanding of the issues. The Committee also wishes to acknowledge the comprehensive research support provided throughout this Inquiry by John Arnol.

Finally, as always, the Committee is indebted to the sterling efforts of its permanent staff, Michele Cornwell and Frances Essaber.

Bill Forwood
Chairman
Public Accounts and Estimates Committee

Executive Summary

Chapter 1 Introduction

The Year 2000 problem is caused by an error in the date recognition code of most computers and their software applications. The effect is not confined to computers – any device using a date-dependent computer chip to control plant and equipment may fail the date test. Such chips are widely used and may be easily overlooked, making the risks particularly pervasive and difficult to quantify. Computers and electronic date-dependent devices with the problem will not recognise the transition to the next century and may stop, malfunction or produce incorrect results.

The Year 2000 problem is significant because it will manifest simultaneously at a multitude of locations and in a wide variety of circumstances. In addition, date-related problems are expected to progressively occur throughout 1999. Due to the interdependencies between computer networks, electronic date-sensitive devices and the main infrastructure systems, small isolated problems may commence a sequence of events that could have serious and widespread consequences for the government, the community and the private sector.

The Year 2000 problem is recognised worldwide as a major risk to both the public and private sectors. It has the potential to have major economic and social ramifications. The Victorian Government, from a public policy point of view, and also as the State's largest business, has a major role to play in ensuring that business critical systems provided by public sector and private sector organisations are compliant.

As government agencies face enormous challenges in coping with the Year 2000 problem, the Committee surveyed all government agencies to assess the following key issues:

- the level of awareness of the Year 2000 problem, particularly at the corporate level of government agencies;
- whether the risks of the Year 2000 problem have been identified, assessed and given appropriate priority by agencies and central government;
- the total costs of managing the Year 2000 problem and whether sufficient funds are available to address major risks to business critical systems;

- the adequacy of planning within the Victorian public sector and whether contingency plans have been prepared to ensure business continuity in the year 2000;
- the implementation, management and monitoring strategies adopted at both the central government and individual agency levels; and
- the legal implications and potential exposure of the Government to legal liabilities arising from the Year 2000 problem.

The Committee found that the Year 2000 problem is unavoidable and that the full extent of its impact on Victoria, indeed throughout the world, is indeterminate.

The Committee's analysis of the progress made by the Victorian public sector in meeting Year 2000 compliance is largely based on the responses received from 244 agencies[4]. The Committee also took evidence from a number of agencies responsible for the maintenance of essential infrastructure systems such as electricity, telecommunications, gas and water supply.

The Committee notes that survey responses and evidence taken present a "snapshot" of the situation in the Victorian public sector between March and July, inclusive, 1998.

Since the announcement of the Committee's Inquiry, the State Government has taken a number of initiatives to ensure agencies adopt a more systematic and structured approach. Significant progress has been made in identifying, ranking and remediating Year 2000 problems.

The Committee particularly welcomes the decision that the Cabinet will receive a report every two months on each agency's progress towards achieving Year 2000 compliance.

The Commonwealth Government has also implemented strategies, many of which are referred to in this report, to address cross-jurisdictional matters and to increase awareness of the problem within government agencies and also in the private sector.

The Committee concludes that addressing the Year 2000 problem in time will be a challenge for the State Government. There is little time left and an increasing scarcity of resources available to individually check and possibly replace the millions of computer chips and lines of computer code, which may malfunction before, on or after 1 January 2000.

[4] The Committee surveyed 445 agencies and received 296 responses, representing a response rate of 67 per cent. Of the 296 agencies, 244 were affected by the Year 2000 problem.

Chapter 2 Awareness of the Year 2000 Problem

Awareness of the scope and nature of the Year 2000 problem is fundamental to preparing an appropriate response to the problem. The Government first issued its Year 2000 Policy to all Departments and public sector agencies in July 1996. The Minister for Information Technology and Multimedia also assigned responsibility for achieving Year 2000 compliance to individual Department Secretaries and agency chief executive officers.

The results of the Committee's survey show that 82 per cent of respondent agencies are affected by the Year 2000 problem and that only 25 per cent of these agencies had commenced their Year 2000 compliance plan by June 1997. Most agencies, however, had commenced compliance activities by late 1997 to mid-1998.

The Committee believes that the public sector's slow response to the Year 2000 problem was caused by a lack of awareness about the nature and scope of the problem and the view that it was the responsibility of the IT section alone to manage. More recently, the Year 2000 problem has been viewed as a far more significant business and risk management problem that will have serious ramifications, if not resolved.

Overall the Committee found that:

- the Year 2000 problem is well understood at the corporate level across the Victorian public sector. Most of the agencies surveyed had developed detailed compliance plans and were focusing their activities on converting or replacing non-compliant operational systems or processes which are critical to business continuity and the performance of core functions or activities;
- awareness of the ramifications of the Year 2000 problem for individual government agencies is also well understood by the staff involved in addressing the Year 2000 issue. Most agencies had given appropriate priority and corporate support to addressing the Year 2000 problem;
- most government agencies are also aware of the potentially damaging impact of non-compliant IT systems which interface and exchange data with other parties' computers as part of normal business activity. Year 2000 compliance activity in this area is less advanced across most government agencies and could potentially pose risks to business critical systems; and
- the impact of embedded chip technology on operational continuity is also well understood across the Victorian public sector. However,

agencies have placed less focus on this aspect of the Year 2000 problem.

The Committee found that many government agencies, however, are unaware of the following important Year 2000 issues:

- the need for a clear 12 months in which to rigorously test and remedy problems that may be found in new IT systems and application programs;
- the need to develop contingency plans and update disaster recovery plans for all modified IT business critical systems;
- the capacity of non-compliant embedded chip technology to affect important environmental and production control functions such as heating and cooling or plant control; and
- programming errors in modified systems will require sustained Year 2000 compliance activities that may extend well into the Year 2000.

From a whole of government perspective there is a need to:

- establish government-wide priorities to remediate systems based on such critieria as the potential for adverse effects on health and safety, business continuity, security and the economy. Further, individual agencies have identified non-compliant systems that are not business critical. Unless priorities are clearly set, the current strategy may divert resources from the most vital government services;
- develop a comprehensive picture of the State's Year 2000 readiness;
- develop Year 2000-related disaster relief planning in the possible event of multiple and concurrent failures in essential services such as telecommunications and utilities i.e. electricity, water and sewerage;
- raise the community's awareness of the Year 2000 problem by reporting on Year 2000 problems and give the required assurances that action is being taken to address these issues;
- develop, in conjunction with the Commonwealth Government, new initiatives to ensure that SMEs undertake contingency planning;
- seek assurances from third parties that any interfacing data systems are Year 2000 compliant. Agencies also need to address this potential risk exposure in their contingency plans; and
- encourage major utility companies and public corporations to share information and coordinate their individual Year 2000 compliance programs in order to ensure Year 2000 compliance in essential services.

In conclusion, the Government's initial Year 2000 strategy accentuated the responsibility of individual departments and other public sector agencies to achieve Year 2000 compliance within the given time frame. This focus was at odds with the need for a risk management overview of the Year 2000 problem. Since the commencement of its inquiry, however, the Committee found that there has been an improvement in the level of awareness through the establishment of a central risk management approach for all public agencies.

In the time available the government must address the potential consequences of the Year 2000 problem for the wider community, especially in terms of preparing contingency plans for business critical systems which may not be compliant.

Chapter 3 Risks Associated with Year 2000

Most government agencies are cognisant of the direct risks associated with the Year 2000 problem for their individual business and business critical systems. Individual agencies have also acknowledged and, in some cases, assessed the risks of the Year 2000 embedded chip technology problem on business continuity.

The Year 2000 Risk Management Unit, the central agency responsible for reporting and monitoring compliance in the public sector, has not been charged with conducting a risk assessment from a whole of government perspective. The wider ramifications of the Year 2000 problem for the community, therefore, are either not as well understood or not well communicated from a whole of government perspective.

The Committee addressed the risk of Year 2000 on a whole of government basis by assessing the results of its Year 2000 survey, evidence gathered from witnesses to the Inquiry and the perceived quality of public sector Year 2000 compliance plans.

From the Committee's analysis the greatest risks at a whole of government level are concentrated in the areas of essential infrastructure systems, small to medium enterprises (SMEs) and hospitals. During 1999, the government must give the highest priority to addressing Year 2000 problems in these critical areas.

Chapter 4 Total Costs of Achieving Year 2000 Compliance

Solving the Year 2000 problem is very costly as it entails labour intensive solutions and time-consuming investigations at several levels. Most large government agencies have approached the Year 2000 problem by re-programming computer code and/or replacing IT equipment (hardware) or

applications (software). These strategies require extensive testing to ensure that such modifications have not introduced problems in what was an otherwise stable IT operating environment. The Committee found that the extensive testing programs needed, which generally cost more than the initial modification, may increase the estimated total cost of agencies' Year 2000 compliance plans.

The Committee's Year 2000 survey results show the total estimated cost of achieving Year 2000 compliance across two-thirds of the Victorian public sector to be in excess of $340 million. The bulk of these funds is to be provided from within existing departmental budgets. This figure compares to $600 million for Commonwealth public sector agencies and $4 billion for the top 150 Australian companies.

Over a third of respondent government agencies had not incurred any expenditure on Year 2000 compliance projects as at 30 June 1998. This figure includes 49 per cent of public hospitals and 75 per cent of public sector superannuation funds. The Committee notes, however, that a significant part of the remediation effort in the public sector is covered by the normal replacement of hardware and upgrade of software and does not appear as a separate expense.

In July 1996 the State Government made additional funds of $600,000 per annum available to Multimedia Victoria to undertake a central Year 2000 policy coordination role. These funds were transferred in July 1998 to the Year 2000 Risk Management Unit, which became the central coordinating body for public sector compliance projects. Since 1997 hospitals have received an additional $3.5 million for the appointment of Year 2000 Project Coordinators and to repair or replace non-compliant embedded chip devices found in hospital medical equipment.

The government has made a commitment to provide additional funds to agencies that are unable to finance business critical Year 2000 compliance areas from within their existing budgets.

Chapter 5 Adequacy of Planning in the Public Sector

The most important aspect of planning for Year 2000 compliance is early commencement. Best practice dictated the commencement of planning for Year 2000 compliance in 1996 with the aim of project completion by 31 December 1998. The Committee's survey show that only a few, mainly small public sector agencies, started planning for Year 2000 compliance in 1996 as required by the Government's Year 2000 Policy.

The survey results show that the majority of public sector agencies commenced planning Year 2000 compliance activities between July and

December of 1997. A significant number of public hospitals and ambulance services (36 per cent), regional water authorities (35 per cent), local councils (33 per cent) and TAFE institutions (40 per cent) commenced Year 2000 compliance activities in March 1998. The Committee notes that VicRoads, Public Transport Corporation and the Metropolitan Fire Brigade only commenced addressing the Year 2000 problem in 1998.

Less than half of the agencies surveyed expect to complete Year 2000 compliance by the end of 1998 and 30 per cent of the agencies were still at the planning and assessment phases of the Year 2000 compliance process. The Minister responsible for the government's Year 2000 program, however, expects all business critical systems to be compliant by 31 December 1998[5].

The central coordination of the whole of government risk management strategy did not commence until August 1998, with the first report to Cabinet made by the Year 2000 Risk Management Unit in September 1998.

Due to the late commencement by the majority of government agencies in addressing the problem, the focus of the government's Year 2000 compliance strategy should be on ensuring the security of essential services and the preparation of contingency plans for all business critical systems.

Chapter 6 Implementation, Management and Monitoring

From the legal and risk management perspectives the quality of the implementation, management and monitoring activities for Year 2000 compliance by public sector agencies will be critical in the year 2000. If well managed, the impact of the Year 2000 problem on government service provision will reduce the Government's exposure to legal liabilities.

The Committee's survey revealed that, during the first half of 1998 most public sector compliance activity (62 per cent) was in the planning and assessment phases.The survey also showed that 77 per cent of agencies believe that their Year 2000 compliance plans are on schedule.

The Committee also examined the preparedness of the essential infrastructure services provided by the electricity, gas, telecommunications and water utilities. All utility agencies gave evidence that they were confident that compliance would be achieved by the Year 2000. One aspect noted by the Committee was the lack of confidence each agency expressed about the preparedness of the other utilities. The Committee has recommended therefore greater communication between interdependent utilities as well as within each industry.

[5] Hon. Roger Hallam, Minister for Finance, PAEC Budget and Estimates Hearing, 27 July 1998, p.37

The Regulator-General plans to introduce an independent reporting framework in 1999 to confirm the Year 2000 status for the electricity industry. Other coordination mechanisms are also being established to enable the sharing of common solutions across the hospitals, water authorities, electricity utilities and local government.

The Committee believes that where agencies are unable to internally fund remediation for business critical systems, additional support from the government should be available. This support should be made available according to whole of government priorities. The Committee believes that those programs delivering emergency services, acute health and public utility services should receive the highest priorities.

The Committee found that there is an important role for auditors to monitor and report on the processes and expenditures undertaken by agencies on Year 2000 compliance programs. Although qualified IT auditors are also needed to verify the Year 2000 remedies implemented by agencies, the Committee notes that there is a reluctance by auditing firms to undertake Year 2000 compliance testing.

The Committee found that project management has been well supported by the executive of each agency and generally well planned. Most agencies have established critical project milestones and expect to meet their project deadlines. Approximately a third of respondent government agencies, however, may not achieve Year 2000 compliance in non-critical areas in the required time due to the lack of a project implementation framework.

The expected shortage of external IT skills in 1999 needs to be addressed and appropriate strategies put in place to ensure the retention of key staff.

Chapter 7 Service Agreements and Contracts

The Committee reviewed the specific warranties and indemnities that are required to be included in all Government purchasing contracts for IT goods and professional IT services. The Committee received legal advice that the model clauses and other contractual provisions offer either no specific protection from potential Year 2000 legal action or only limited protection.

In any case, the Committee was informed by a number of witnesses that most agencies had failed to include the required protective contractual clauses in their IT purchasing agreements.

The Committee notes that some very large service agreements under the Government's recent privatisation and outsourcing programs do not have any specific protection or indemnities relating to the Year 2000 problem. The Committee understands that some of these contracts have been

renegotiated and amended to require the current contractors to remediate the Year 2000 problem, but at significant extra cost to the Government.

The central purchasing authority for the Government has recently commenced a number of initiatives that address the matters raised in the Committee's review of IT service agreements and contracts. These include a requirement for all Year 2000 compliant service providers and vendors of IT equipment to centrally register their businesses on an Internet Web site. Agencies will be advised to only select those IT vendors and professional services registered on the Government's web site.

The Committee concludes that the Government is exposed to potential losses arising from non-compliant IT equipment or under-performance by professional IT service providers.

Chapter 8 Legal Implications

The legal implications of the Year 2000 problem are as vast as the nature of the Year 2000 problem itself. The economic, social and environmental impacts of the Year 2000 problem may lead to litigation against government agencies and directors of companies for damages arising from negligence, breach of contract, consumer protection, and occupational health and safety issues.

The potential social, economic and environmental impacts of the Year 2000 problem, global in scale and pervasive in nature, are unprecedented. It is now critical for the Government to directly intervene to encourage the co-ordination of risk assessment and management activities in both the private and public sectors. For example, additional measures to increase the flow of information between parties are needed and should include:

- legislation to encourage the sharing of information between all parties involved in the resolution of the Year 2000 problem;
- legislation to compel private and public sector entities to fully disclose the status of their Year 2000 preparedness; and
- the establishment of a team of technical experts to independently confirm the progress of Year 2000 compliance activities in business critical systems and with other essential service providers.

The Committee found a potentially high level of exposure to Year 2000-related legal action for damages or losses in Government service agreements entered into by agencies since 1996. Several large contracts with major IT vendors have also left the Government exposed to additional costs due to Year 2000 compliance requirements.

The Victorian Government Purchasing Board is currently increasing its Year 2000 compliance standards for private sector companies that supply goods or services to Government agencies. All private sector companies that tender for Government contracts will need to be Year 2000 compliant or at least be able to demonstrate their compliance programs.

The survey results indicated that half of the agencies surveyed did not retain any documentary evidence of real life testing conducted on Year 2000 compliant systems. The Committee is concerned that such lack of documentation may leave agencies exposed in the event of litigation concerning negligence.

Chapter 9 Community Assurances

The Committee found three additional issues that need to be addressed by the Government:

- the need to develop partnerships with industry groups to assist in the Year 2000 effort in the private sector, particularly with SMEs;
- the need to strengthen community assurances through the development of a Public Confidence Program containing strategies on how to communicate key information about the compliance status of essential services and the most probable impacts of the Year 2000 problem; and
- the need to dispel any notions of a doomsday scenario by regularly reporting to the Parliament on the Year 2000 problem.

Public sector respondent agencies have generally achieved best practice as measured against the ICA guidelines, however, the late start now warrants that the Government gives this issue a high priority. Resources must be directed towards the compliance of essential infrastructure services, hospitals, utilities and emergency services. All agencies need to prepare contingency plans to ensure at least minimum levels of service will be available in a worst case scenario.

The State Government, local councils, industry and business groups and community groups all have a key role to play in preparing Victoria for the Year 2000 problem.

The Committee does not underestimate the challenge offered by the Year 2000 problem but it is reassured that the government has taken a number of initiatives to minimise the risk posed to the operation of government from the 1999-2000 date roll-over.

RECOMMENDATIONS

Chapter 1: Introduction

The Committee recommends that:

Recommendation 1.1: page 10

The government:

- ***respond to the recommendations contained in this report during the autumn session of Parliament;***
- ***outline the timetable for the implementation of the recommendations;***
- ***report on progress against these timelines; and***
- ***response form part of the broader report to the Parliament on the government's year 2000 strategy.***

Chapter 2: Level of Awareness of the Year 2000 Problem in Victoria

The Committee recommends that:

Recommendation 2.1: Page 21

To expedite corrective efforts, those agencies which have not commenced compliance projects, be directed by the government to commence immediately and to publish details of the commencement dates in the report to the Parliament on the Year 2000 problem in the autumn session of 1999.

Recommendation 2.2: page 22

The government develop and implement a new public awareness campaign for the public sector and the community clearly outlining what the Year 2000 problem is, the consequences of non-compliance, what aspects of service or business operations it may affect, sources of information and assistance and stressing the need for immediate action.

Recommendation 2.3: page 22

An objective of the campaign be raising awareness of the various levels of risk for business continuity.

Chapter 2: Level of Awareness of the Year 2000 Problem in Victoria *(continued)*

The Committee recommends that:

Recommendation 2.4: page 22	***The awareness campaign be aimed at educating a wide audience of the need for contingency planning.***
Recommendation 2.5: page 22	***The awareness campaign be in plain language and avoid the use of terms or images that depict a "bug".***
Recommendation 2.6: page 23	***The Department of State Development liaise with peak industry bodies and organise industry forums to facilitate the sharing of information on common problems and solutions. These industry groups should be involved in identifying critical problems and assist in developing industry-wide contingency plans.***
Recommendation 2.7: page 23	***Greater awareness be made of the problems that can occur due to the interconnectivity of business systems and the probable manifestations of the Year 2000 problem that will occur in all date-dependant embedded chip technology.***
Recommendation 2.8: page 23	***Agencies distribute information on a regular basis, to staff and customers in order to build commitment and to communicate progress on Year 2000 compliance.***
Recommendation 2.9: page 23	***There is sharing of information on best practices for dealing with the Year 2000 problem amongst public sector agencies and between public and private sectors.***

Chapter 3: The Risks Associated with Year 2000

The Committee recommends that:

Recommendation 3.1: page 31	***The Year 2000 Risk Management Unit assess the need for further compliance work in public sector agencies which have yet to account for the potential effects of the Year 2000 problem on business continuity and service quality.***
Recommendation 3.2: page 31	***Priority be given to the development of interchange standards if the Year 2000 data interface problem is to be resolved before 31 December 1999.***
Recommendation 3.3: page 34	***The government determine whole of government priorities for remediating business critical systems based on such criteria as the potential for adverse health and safety effects, adverse financial effects on the community, detrimental effects on security and adverse economic consequences.***
Recommendation 3.4: page 34	***The government assess the State's Year 2000 risks, including those posed by key economic sectors.***
Recommendation 3.5: page 34	***The Year 2000 Risk Management Unit build and maintain close links with the essential infrastructure organisations in order to be aware of the status of Year 2000 compliance programs.***
Recommendation 3.6: page 34	***Businesses and departments be encouraged to identify areas where a manual backup should be considered as part of their contingency planning.***

Chapter 3: The Risks Associated with Year 2000 *(continued)*

The Committee recommends that:

Recommendation 3.7: page 35	***To ensure that risks are minimised in the interests of patient safety, the Department of Human Services assess the readiness of public and private hospitals and medical facilities for the Year 2000 problem.***
Recommendation 3.8: page 35	***The Office of the Regulator-General assess and report to Parliament on the Year 2000 readiness of all electricity generation and distribution units and the potential impact of the Year 2000 problem on the transmission system.***
Recommendation 3.9: page 35	***The Bureau of Emergency Services Telecommunications assess the impact of the Year 2000 problem on the emergency response systems that are dependent on the Global Positioning System satellite system and emergency radio, microwave communications systems and computer aided call and dispatch systems.***
Recommendation 3.10: page 35	***The Police, the Country Fire Authority and the Metropolitan Fire and Emergency Services Board undertake an awareness campaign so that property owners have all security and fire alarms Year 2000 compliant by July 1999.***
Recommendation 3.11: page 35	***The Department of Natural Resources and Environment assess the readiness of all water authorities and waste water treatment facilities for the Year 2000 problem. The Department make known problems and potential solutions for specific vendor-supplied systems and equipment.***

Chapter 3: The Risks Associated with Year 2000 *(continued)*

The Committee recommends that:

Recommendation 3.12: page 36	***That the Victorian WorkCover Authority, in light of its responsibilities under the Occupational Health and Safety Act 1985 and the Dangerous Goods Act 1985, seek assurances from all licensees that they will be Year 2000 compliant and follow-up and assess those responses and report on this matter to the Parliament in the autumn session 1999.***
Recommendation 3.13: page 36	***The Office of Corrections assess the impact of the Year 2000 problem on security and environmental control systems in prisons.***

Chapter 4: The Cost of Achieving Year 2000 Compliance

The Committee recommends that:

Recommendation 4.1: page 43	***The government make it more widely known, particularly to SMEs, that the cost of the Year 2000 problem represents the cost of staying in business.***
Recommendation 4.2: page 43	***The government allocate priorities across all agencies for Year 2000 funding commitments according to a risk assessment undertaken by the Year 2000 Risk Management Unit.***
Recommendation 4.3: page 43	***In the event that key agencies are unable to meet the cost of compliance for business critical systems from within their budget, the government allocate the required funding.***

Chapter 4: The Cost of Achieving Year 2000 Compliance *(continued)*

The Committee recommends that:

Recommendation 4.4: page 43	***As a means of monitoring the achievement of year 2000 compliance, the government track agencies' expenditure against year 2000 compliance plans.***
Recommendation 4.5: page 43	***Agencies' annual reports include information on their total year 2000 expenditure and the sources of all internal and external (i.e. Advance to the Treasurer) funds.***

Chapter 5: Adequacy of Planning for the Year 2000 Problem

The Committee recommends that:

Recommendation 5.1: page 52	***The government establish spot checks by appropriately qualified auditors on the progress of all essential infrastructure service providers against Year 2000 compliance targets.***
Recommendation 5.2: page 52	***If it becomes apparent that some business critical systems will not be fully compliant by key dates, government ensure that adequate contingency plans are developed and tested[6] to guarantee business continuity and the continuation of government service provision.***
Recommendation 5.3: page 52	***The government focus on critical areas where planning and progress to date shows that improvement is needed.***
Recommendation 5.4: page 52	***The State's disaster response plan (DISPLAN) be reviewed to take into account the possibility of simultaneous disasters arising from the Year 2000 problem.***

[6] The Committee is aware of community Year 2000 simulation exercises conducted in the US. For example, in Lubbock, Texas, in *The Australian*, 6 October 1998, p.5.

Chapter 6: Implementation, Management and Monitoring Strategies

The Committee recommends that:

Recommendation 6.1: page 66	***The government expand the 'spot checking' audit function of the Year 2000 Risk Management Unit to focus its verification reports on the essential services – gas, water, electricity, emergency communications and the major hospital networks.***
Recommendation 6.2: page 66	***As a matter of priority, resources be made available to enable business critical systems to be made compliant. Contingency plans need to be coordinated across the hospital system to cater for all emergency eventualities.***
Recommendation 6.3: page 66	***To encourage the sharing of information, the appropriate agency organise forums for agencies and industries that are likely to share common Year 2000 problems e.g. the emergency services, SMEs, water, gas and electricity retailers and distributors, electricity generators and transmission companies.***
Recommendation 6.4: page 66	***That similar agencies such as those in local councils or water management authorities be encouraged to share IT resources for remediating common Year 2000 problems.***
Recommendation 6.5: page 66	***Agencies verify whether their contingency plans are sufficient to ensure business continuity and the maintenance of adequate levels of service in the event of multiple failures.***
Recommendation 6.6: page 67	***The annual report data on Year 2000 compliance activities for 1997-98 be centrally collated by the Year 2000 Risk Management Unit as a means of measuring the progress of public agencies since the Public Accounts and Estimates Committee survey.***

Chapter 6: Implementation, Management and Monitoring Strategies *(continued)*

The Committee recommends that:

Recommendation 6.7: page 67
All agencies thoroughly test new IT systems and IT equipment under real life conditions to ensure the proper completion of year 2000 compliance activities.

Recommendation 6.8: page 67
The Government develop IT staff retention strategies to ensure the retention of IT personnel with the appropriate skills for year 2000 related work.

Chapter 7: Service Agreements and Contracts

The Committee recommends that:

Recommendation 7.1: page 75
All agencies review existing contracts with particular consideration to the following matters:
- ***warranties that services and products are intended to function beyond 1999;***
- ***the drafting of specifications;***
- ***any exclusions or limitations on liability; and***
- ***indemnities.***

Recommendation 7.2: page 76
Agencies include the GITC3 clause in all relevant contracts, not just IT contracts.

Recommendation 7.3: page 78
The government immediately advise all government suppliers that year 2000 compliance is a requirement before they can enter into contract agreements with government agencies.

Recommendation 7.4: page 78
Compulsory labelling of all IT equipment be introduced to indicate year 2000 compliance e.g. with the Standards Association of Australia/Standards New Zealand Year 2000 compliance standards.

Chapter 8: The Legal Implications of the Year 2000 Problem

The Committee recommends that:

Recommendation 8.1: page 85	***Agencies review the potential year 2000 failures that may affect their capacity to fulfil their contractual, community and legal obligations. Reviews should include an assessment of the impacts of any year 2000 failures on suppliers of goods and services i.e. liability for failure on the part of the agency, and any organisation on whom the agency is dependent or inter-reliant.***
Recommendation 8.2: page 94	***The Victorian Government give urgent consideration to introducing Good Samaritan legislation in Victoria to encourage the dissemination of information regarding year 2000 preparedness and compliance issues.***
Recommendation 8.3: page 94	***The government introduce Good Samaritan legislation in isolation of a national approach, if necessary.***
Recommendation 8.4: page 94	***The proposed Good Samaritan legislation should:*** • ***be clear that pooling of information on the Year 2000 problem does not constitute anti-competitive conduct under the provisions of the Trade Practices Act;*** • ***provide clear incentives for information disclosure through limiting legal liability arising on the basis of such disclosures;*** • ***establish clear principles for effective information disclosure; and*** • ***have broad coverage but not alter consumer protection laws.***

Chapter 8: The Legal Implications of the Year 2000 Problem *(continued)*

The Committee recommends that:

Recommendation 8.5: page 96

In terms of copyright issues, agencies take the following actions:

- ***all software currently in use be identified and the terms affecting its use be clarified;***
- ***identify software which has a Year 2000 problem;***
- ***identify copyright owners who offer to make their software year 2000 compliant and the terms and conditions of the offer; and***
- ***the written permission of the copyright owner is sought where the copyright owner offers no solution and modification is needed.***

Recommendation 8.6: page 96

The government make representations to the Commonwealth Government for the urgent amendment of the Copyright Act to:

- ***exclude the reproduction of a program solely for the purpose of assessing year 2000 compliance from infringement; and***
- ***permit modifications to software to remedy a Year 2000 problem. This exception may be absolute or subject to a reasonableness requirement such as granting the copyright owner the right of first refusal of repair, on reasonable terms and within a reasonable time.***

Recommendation 8.7: page 98

The government ensure that all public sector managers are made aware of the legal liabilities of non-compliance.

Chapter 8: The Legal Implications of the Year 2000 Problem *(continued)*

The Committee recommends that:

Recommendation 8.8: page 99	***Agencies commence internal audits to identify potential areas where year 2000 liabilities may arise. The internal reviews identify potential year 2000 failures that may affect the government's capacity to fulfil its contractual, community and legal obligations.***
Recommendation 8.9: page 99	***Internal reviews also include an assessment of the impacts of any year 2000 failures on persons who supply goods and services to government, ie. liability for failure on the part of the government and any organisation or dependent or inter-reliant entity.***
Recommendation 8.10: page 99	***All agencies thoroughly document their year 2000 compliance activities to establish an audit trail to show that best efforts and due diligence had been taken.***
Recommendation 8.11: page 99	***The government emphasise to all agencies the importance of retaining documented evidence of all year 2000 activities including all results of real life tests.***
Recommendation 8.12: page 99	***Agencies develop strategies to protect against the occurrence of any identified liabilities.***
Recommendation 8.13: page 99	***All agencies develop disaster recovery plans for business critical systems and that this be considered an aspect of any year 2000 disclosure legislation.***

Chapter 9: Community Assurances

The Committee recommends that:

Recommendation 9.1: page 106	***The government report by 31 January 1999 on the status of its objective for all business critical systems in the public sector to be compliant by 31 December 1998.***
Recommendation 9.2: page 106	***The government ensure adequate resources are directed towards the compliance of essential infrastructure services, hospitals and the emergency services.***
Recommendation 9.3: page 106	***The government promote greater awareness in SMEs of the Year 2000 problem and of the need for the development of appropriate contingency plans to ensure business continuity in the year 2000.***
Recommendation 9.4: page 106	***The government advise local government and the Victorian community of the State's priority areas for Year 2000 compliance.***
Recommendation 9.5: page 106	***The government develop a Year 2000 Public Confidence Program containing strategies on how to communicate key information about the compliance status of community services and possible impacts.***
Recommendation 9.6: Page 107	***The government establish a Help Line and an organisational network of both public and private sector IT experts, which can provide assistance in the time leading up to the Year 2000.***

Chapter 9: Community Assurances *(continued)*

The Committee recommends that:

Recommendation 9.7: page 107	***The government establish a Community Contingency Planning Group through the Disaster Planning Organisation, the State Emergency Management Council, local councils and relevant community organisations, to plan for potential problems.***
Recommendation 9.8: page 107	***The government establish by 30 November 1999 Communication and Incident Centres together with a year 2000 emergency call number.***
Recommendation 9.9: page 107	***The government develop a year 2000 policy that provides that government agencies will not continue electronic business dealings with private sector companies that do not have year 2000 compliant computers.***

Chapter 1: Introduction

"…Year 2000 could force a whole lot of things to happen together" [7]

1.1 Background to the Inquiry

The Victorian Auditor-General in the May 1997 *Report on Ministerial Portfolios,* reported that the potential liabilities and risks in relation to the Year 2000 issue were not well understood across the public sector and that government agencies may not be well-positioned to deal with the impending Year 2000 problem. At the request of the Auditor-General, the Public Accounts and Estimates Committee resolved on 13 February 1998 to undertake an inquiry into information technology and the Year 2000 problem and the level of preparedness of the Victorian public sector. The Committee believes that the conduct of this inquiry itself has contributed to a greater awareness of the issue.

1.2 What is the Year 2000 problem?

Historically, a wide range of electronic control systems in computers, software applications and other devices represent the year of any date by its last two digits (e.g. 1998 is recorded as 98). The century was not entered. Systems were programmed in this way to reduce data entry time, economise on memory requirements and to save processing time.

It is now widely acknowledged within the computer industry that date-sensitive systems may not correctly distinguish between the years of any particular century (e.g. whether a year is in the 1900s or 2000s). As a result, at the beginning of the next millennium some systems may shut down, malfunction or simply fail to operate as designed. Other information technology systems and applications may produce meaningless data or default to some base date.

To change all systems involving computers and microcomputers so that they accept a four-digit year date format is an enormous task. Practically every single automated system and its related technology, regardless of size, is impacted. Many of the in-house, legacy systems are relatively old and are written in computer languages no longer in use. Some applications include thousands, tens of thousands, or even millions of lines of code, each of which must be examined for date-format problems. There is no single solution, even where the same date-related problems are identified in

[7] Ms. W. Auchincloss, Information Manager, Melbourne Water, PAEC Private hearing, 28 August 1998.

similar items of plant and equipment, every computer program or chip must be individually checked. Further complications arise when government agencies and the private sector have to modify their programs while still undertaking their current activities. These challenges are collectively referred to as the Year 2000 problem.

1.3 Why is the Year 2000 problem significant?

The Year 2000 factor can cause a problem to occur at any time up to, including and beyond the year 2000. If not rectified, the problem may disrupt a wide range of systems and business processes on which agencies and the private sector heavily depend. Problems are expected to progressively occur in 1999 in all non-compliant computer systems that, for example, project data into 2000 to forecast budgets, investment returns, superannuation liabilities or other financial and technical matters.

The full extent of the Year 2000 problem is unknown. The effect is not confined to computers; any device using a date dependent computer chip to control plant or equipment may fail the date test. These embedded chips are widely used and may be easily overlooked, making the risks particularly pervasive and difficult to quantify.

The Year 2000 problem may affect:

- conventional electronic information systems such as mainframe computers and their applications;
- computer networks, personal computers and the applications running on them; and
- microchips embedded in a vast range of plant and equipment such as electricity generation plants, security systems, telecommunications equipment and networks, medical equipment, air conditioning systems, etc. A full list of devices is included at Appendix 1.

Government agencies are also likely to be exposed to additional risks arising from their business relationships with external parties who rely on the exchange of date-sensitive data. For example, many outsourced services such as pay roll and patient data services exchange date-sensitive data with government computers as part of service agreements. If the computer systems of the contractor are not Year 2000 compliant they may corrupt the existing databases in an agency's computer systems.

Some specific dates of expected Year 2000 problems are shown in Exhibit 1.

Exhibit 1

DATES ON WHICH PROBLEMS MAY OCCUR

Date	*Potential problem*
1 January 1999	Computers that calculate dates by looking one year ahead and then calculating backwards, may fail.
1 July 1999	The start of the 1999-2000 financial year. Non-compliant applications that use financial years could fail. Government begins the fiscal year and all financial management systems will need to be compliant.
21 August 1999[8]	Systems in aeroplanes, ships and emergency communications that use Global Positioning Satellites (GPS) to determine location may fail as the satellite systems reset to zero. Impacts in non-synchronised navigation, transportation and mapping systems that are not manually reset to zero.
9 September 1999	Many programmers used to allow users to escape from a program by entering "9999" in a date field. Others used the same entry to indicate the end of a file. On "9/9/99" some old systems will cause problems when the user enters the current date in a date field.
1 January 2000	The new millennium. Computers that read the date as 1 January 1900 may halt, confuse or otherwise disrupt many systems and devices. This day is a public holiday.
4 January 2000	4 January 1980 was the first date registered by MS-DOS. Many non-compliant systems that use MS-DOS may default to this date. Also the first working day after 1 January 2000.
29 February 2000	The rules for calculating a leap year are that the year must be divisible by 4 or 400, but not by 100. 29 February 2000 is a once in 400 years leap day that many programs may not recognise.
30 June 2000	Non-compliant reconciliation programs may begin to fail at the end of the financial year.
10 October 2000	The first time date fields use maximum length. Problems may occur in remediated systems for the first time.
31 December 2000	Some systems may not recognise the 366th day of the leap year. If the computer did not recognise 29 February 2000 there will only be 365 days and the system will crash on the next day.
1 January 2001	Due to the patches used to fix the problem, in 2001 some PCs with Windows 95 will reset back to 1900, or to a default date.
8 September 2001	The Unix operating system counts this date as 999,999,999 and some programs will terminate operations when this date is entered.

[8] This is a date-related computer problem that is not associated with the change in century. The GPS uses a time-keeping system that operates on a 1024 week cycle or "epoch". The current epoch ends on 22 August 1999.

Since the Year 2000 problem pervades all sectors of the Victorian Government's operations and has an immovable deadline, fixing the problem is one of the most comprehensive management and technical projects ever faced. The possible consequences of computer system failures in a vast range of government activities, in areas as diverse as health; public safety; emergency services; water; gas and electricity are very serious.

Hypothetically, in a worst case scenario, society could be faced with:

- simultaneous failure of electricity, gas and water supplies with complications caused by the loss of emergency warning and communications systems;
- concurrent failures in warning alarms (emergency shut down systems) and security systems with simultaneous losses in telecommunications, radio and satellite communications;
- loss of business continuity across wide sections of industry resulting in the loss of supply chains, including food distribution, parts for manufacturing industries; and
- failure of financial systems caused by the loss of accurate data systems, electronic data interchange and financial information systems.

However, the Committee rejects the doomsday scenario. The Committee believes that although it is inevitable that things will go wrong, there is a structure in place that will minimise the impacts of the Year 2000 problem. The Committee is also reassured that the Government has given the Year 2000 problem its highest priority and has made a strong commitment to its resolution. With further appropriate and timely actions, such as those recommended in this Report, the Committee believes these scenarios can be avoided.

Significant systems that Victorian[9] government agencies must ensure are compliant include:

- the computerised emergency response system, which supports the call and dispatch of ambulance, fire, police and emergency services. As well as any medical equipment in the ambulances or hospitals that contain date dependent computer chips;
- the electricity transmission and distribution systems, which include date dependent telemetry devices and SCADA systems;

[9] Commonwealth agencies that are dealing with the Year 2000 problem for other significant services include Telstra (telecommunications), Centrelink (social welfare payments), Reserve Bank (banking system) and the Civil Aviation Safety Authority (air traffic control, navigation)

- the gas distribution system which also include remote telemetry monitoring devices and central SCADA systems;
- water delivery and treatment systems, which have automated processes for water treatment and pressure/flow controls;
- building control systems for air conditioning and ventilation which include automated HVACS systems;
- transportation and traffic control systems that govern signaling systems for trains, trams and major intersections; and
- the revenue collection systems for the government.

It is a major challenge just to identify which systems and technology are affected and to determine the extent of their impact. The next steps are equally important, to develop appropriate strategies, to obtain the required resources and expertise, to provide sufficient testing and to implement corrective action within the time frame allowed.

The State Government is not alone in facing this problem. Businesses and organisations around the world also face the Year 2000 threat. In Australia consultants estimate that the Year 2000 effort will cost Australian companies $10 billion[10] to correct, State and Federal governments over $1 billion[11] and the Australian economy over $12.5 billion and the loss of 350,000 jobs if only ten per cent of small businesses fail to deal with the problem.[12]

In the private sector, many large firms such as major banking institutions have been actively addressing the Year 2000 problem, but many other businesses have not commenced to address the problem. One economist[13] has predicted a worldwide recession due to the effects of widespread business failures that may result from the Year 2000 problem. The risks are particularly high for small and medium sized businesses, where the potential impact of Year 2000 may not be fully appreciated. Should a high rate of business failure occur,[14] it could have a detrimental effect on the State's economy, with repercussions for the state's revenue and serious impacts on employment and trade.

[10] Deloitte and Touche Consultants from an analysis of ASX filings as reported in *The Australian*, 22 September 1998, p.33

[11] *The Australian Financial Review*, 1 July 1998, p.33

[12] Mr Maurice Newman, Chairman of the National Year 2000 Steering Committee, *Business Review Weekly*, 23 March 1998;

[13] Chief Economist of Deutche Morgan Grenfell, Dr. Edward Yardeni, estimates a 60 per cent chance of a world-wide recession in 2000, in *The Australian Financial Review*, 23 April 1998, p.46.

[14] The Australian Bankers Association found 69 per cent of SMEs have done nothing to address the Year 2000 problem - In *The Australian*, 26 April 1998, p.33.

The more significant areas in the private sector include the banking and finance sectors, the small and medium businesses that control food production and distribution networks; electricity generation; gas production and the larger businesses including the petroleum and pharmaceutical industries.

1.4 The Inquiry process

The terms of reference adopted by the Committee were to:

- assess the level of awareness of the Year 2000 problem in the Victorian public sector;
- review the risks associated with the Year 2000 problem;
- determine the total costs expected to be incurred by the Victorian public sector to ensure that it is Year 2000 compliant;
- review the adequacy of planning within the Victorian public sector for the achievement of Year 2000 compliance;
- review the implementation, management and monitoring strategies for Year 2000 compliance; and
- determine whether the Year 2000 problem has been addressed in service agreements and contracts**.**

The following Sub-Committee was appointed to conduct this inquiry:

Mr S J McArthur, MP (Chairman of this Inquiry)
Hon. W Forwood, MLC (Chairman of the PAEC)
Mr R J Hulls, MP
Hon. T C Theophanous, MLC

The inquiry was advertised in the press on 28 February 1998. Invitations to provide submissions were sent to a range of business organisations, financial institutions and other interested persons. A list of submissions received is at Appendix 2.

1.5 Process followed by the Committee

The Sub-Committee forwarded a detailed questionnaire on the Year 2000 problem to all public sector agencies in February 1998. The questionnaire was designed to assess whether public sector agencies were making adequate progress in addressing and managing the Year 2000 problem. In addition, on 26 February 1998 the Sub-Committee wrote to the Minister for Information Technology and Multimedia, Hon. Alan Stockdale, requesting a submission on the following issues:

- the risks identified from a whole of government perspective;

- the strategies developed to address the Year 2000 problem,[15] from a whole of government perspective and the timetable for implementation;
- the activities across the Victorian public sector that would ensure that all public sector agencies were Year 2000 compliant;
- the roles and responsibilities within and across government for addressing the Year 2000 problem;
- the total expected costs to the Victorian Government to address the Year 2000 problem;
- the funding arrangements for the resolution of the Year 2000 problem;
- the accountability mechanisms implemented by the government to assess agencies' ability to effectively deal with the Year 2000 problem;
- whether consideration had been given to requiring significant agencies/departments to provide certification to government once their systems were Year 2000 compliant;
- whether the government had set a date by which it expected all public sector entities to be Year 2000 compliant;
- whether the government had considered the legal implications of service failures and, if so, to provide the Committee with information on the legal implications of Year 2000 non-compliance;
- whether the government issued a statement to agencies regarding the purchase of Year 2000 compliant products;
- whether consideration had been given to developing an agreement between Federal and State governments on the Year 2000 issue;
- the action taken to ensure the integration of the Year 2000 project with the implementation of IT outsourcing arrangements; and
- the strategies developed to address the limited availability of:
  (a) external consultants with Year 2000 expertise; and
  (b) IT staff with Year 2000 expertise in the public sector.

The Committee was disappointed with the lack of response from the government to the issues raised.

Early in the Committee's inquiry the Government acted to strengthen its approach to the Year 2000 problem. On 7 July 1998 the government

[15]The Sub-Committee similarly wrote to the Minister for Finance, Hon. Roger Hallam, on 16 July 1998- see Appendix 3.

appointed the Minister for Finance as Minister in charge of the government's response to the Year 2000 problem with a brief to:

- coordinate the Government's overall response to the Year 2000 problem;
- report monthly to Cabinet on the Year 2000 status of agencies;
- identify the risks to government and appropriate responses; and
- identify resource requirements to ensure Year 2000 compliance is achieved in critical areas.

The Committee welcomes this further action as evidence that a whole of government approach is being taken to the Year 2000 problem and additional funds will be committed if, and when, required.

The Year 2000 Sub-Committee received evidence on the Year 2000 preparedness of important public infrastructure services at a series of private hearings conducted in Melbourne, Sydney and Canberra between July and September 1998.

All hearings were held *in camera* and assurances given to witnesses that evidence given would not be used in the Committee's report without seeking agreement. This arrangement encouraged witnesses to be more forthright, as the Committee was aware of the high-risk areas and that there was some degree of uncertainty on various legal issues.

Private hearings were also held with the Regulator-General, Dr John Tamblyn; officials of the Commonwealth's Year 2000 National Steering Committee; staff from the Commonwealth Office of Government Information Technology (OGIT); the Manager of the NSW Year 2000 Compliance Unit; Officials from the Reserve Bank and the Australian Prudential Regulation Authority; OGIT's legal adviser on the Year 2000 issue and key officials involved with the Year 2000 problem for business critical systems in the Victorian public sector. A list of the witnesses appears at Appendix 4.

The Committee is very appreciative of the frank and full advice received from the witnesses. Overwhelmingly, there is a realisation that addressing the Year 2000 problem in time will be a tremendous challenge for public and private organisations. While all witnesses were conscious that the Year 2000 problem has the potential to be catastrophic, most were confident that the risks can be mitigated and disruptions minimised if the appropriate strategies are adopted quickly. Many of the recommendations contained in this report are intended to assist agencies in addressing this issue.

1.6 Structure of the report

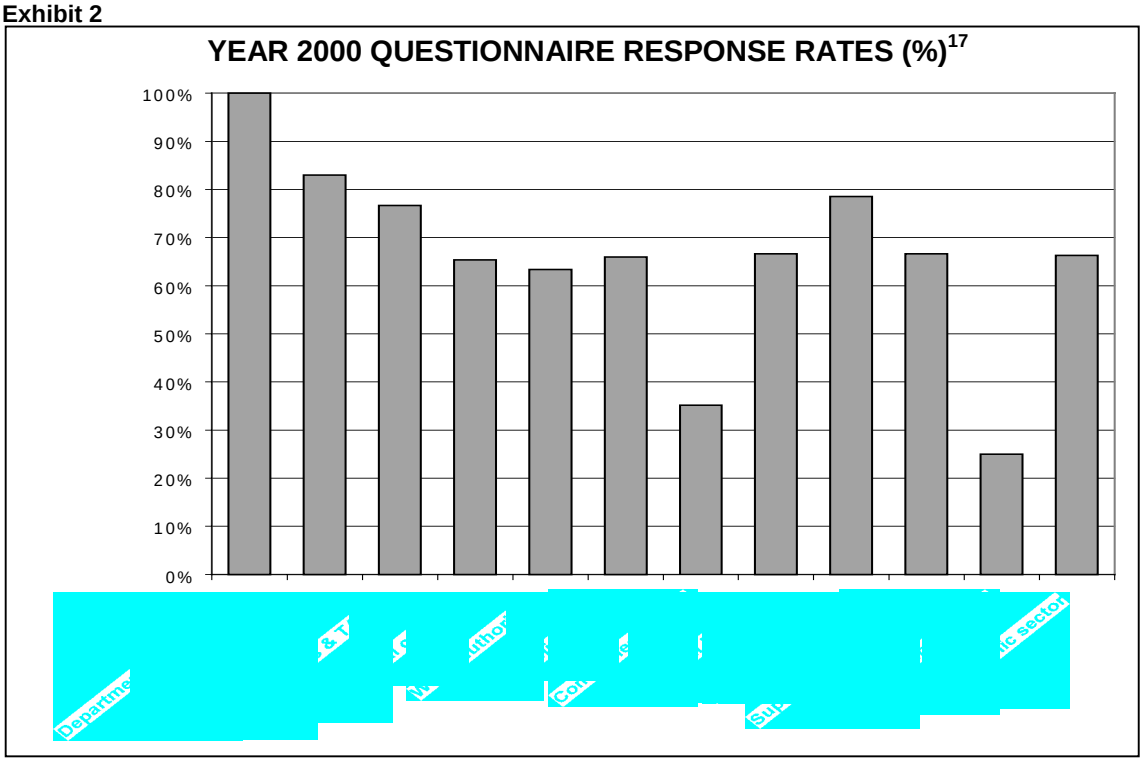
The following chapters of the Report address the terms of reference. Each chapter describes the survey results for various groups of agencies and provides an assessment of the situation as at the date of survey.

In addition, the Committee adopted a multi-level approach in seeking evidence to determine the level of preparedness of the Victorian public sector. Information sources used include:

- each agency's response to the Year 2000 questionnaire;
- private hearings (*in camera*) with witnesses from agencies with critical business systems;
- benchmarking Victorian progress against national and international practice;
- benchmarking agencies against best practice; and
- public submissions.

The Committee's Year 2000 questionnaire '*Information Technology and the Year 2000 Problem: Is the Victorian Public Sector Ready?*' [16] received a good response rate of 67 per cent from government agencies. The information provided a statistically significant result and gave the Committee an indication of the state of preparedness of various agencies in the Victorian public sector for the period 3 March to 31 July 1998.

Exhibit 2



[16] see Appendix 5 - Year 2000 questionnaire survey.
[17] Survey data for the period 3 March 1998 to 31 July 1998

A list of the inner and outer budget agencies that responded to the Committee's questionnaire within each of the above public sector categories, is provided at Appendix 6.

The questionnaire was designed to permit an assessment of the preparedness of the Victorian public sector in terms of the following Year 2000 issues:

- the extent of the Year 2000 problem across all agencies in terms of existing IT hardware, embedded chip systems and applications;
- the major risks of the Year 2000 problem to agencies and clients;
- whether compliance plans have been established and the adequacy of the plans;
- whether task forces have been established and the resources needed;
- the extent of inter-agency connectedness and the levels of cooperation needed;
- the progress of agencies against key project milestones; and
- whether contingency plans have been established.

The Committee first established the approximate state of preparedness of the Victorian public sector then compared the result with progress reported by other jurisdictions both in Australia and overseas.

Specific results of the Year 2000 questionnaire were compared with current best practice in terms of recommended dates for commencing, implementing and completing Year 2000 compliance programs. For example, best practice is to complete all corrective action and testing of changed systems by the end of 1998.

The Committee recommends that:

Recommendation 1.1:	***The government:*** • ***respond to the recommendations contained in this report during the autumn session of Parliament;*** • ***outline the timetable for the implementation of the recommendations;*** • ***report on progress against these timelines; and*** • ***response form part of the broader report to the Parliament on the government's year 2000 strategy.***

Chapter 2: Level of Awareness of the Year 2000 Problem in the Victorian Public Sector

"Up until earlier this year we've had a program of business areas managing their own PC acquisitions…the centralised program is only actually starting now." [18]

2.1 Introduction

The Committee found that lack of awareness of the Year 2000 problem might have contributed to an inadequate initial response by agencies and the government. The Year 2000 problem was initially viewed by government as an IT problem that was best managed by the IT section of each individual agency or department.[19]

Realisation that the Year 2000 problem was a serious business management problem, which required a centrally controlled risk management strategy and a whole of government approach, was first acted on by the government in July 1998.

2.2 Victorian Government initiatives

The Victorian Government first alerted departments to the Year 2000 problem in July 1996 through the issuance of the Year 2000 Policy[20] by the Minister for Information Technology and Multimedia. The Minister also forwarded letters to all Department Secretaries, the Auditor-General and IT directors regarding this policy. The Minister assigned responsibility for Year 2000 compliance to the individual Department Secretaries and the Chief Executive Officers (CEOs) of each public sector agency. Multimedia Victoria was given the responsibility for administering the government's Year 2000 Policy including raising awareness of the Year 2000 problem across the whole of government.

The Committee believes that at July 1996 the "Millennium Bug" was considered by many senior officials to be an information technology problem that could be dealt with on the basis of individual departmental IT initiatives. This observation could explain the low profile with which the Year 2000 problem was held by most agencies until 1998.

---

[18] Mr Colin Jordan, Chief Executive, VicRoads, in answer to a question about whether Year 2000 compliance assurances for PCs were commenced in 1996. PAEC Private hearing, 28 August 1998, p.11.
[19] Hon. Alan Stockdale, Treasurer, Budget and Estimates hearing, 5 May 1998, p.23.
[20] A copy of the Victorian Government's Year 2000 policy is at Appendix 7.

The Victorian Auditor-General in his *Report on Ministerial Portfolios*, May 1997, expressed disappointment at the level of awareness of the Year 2000 problem across the public sector. The Secretary, Department of State Development in his response to the audit report stated:

> "*We agree with the Auditor-General's conclusions and the thrust of the recommendations, however, the window for remedial action is now approaching a point where awareness is not the key issue but rectification is.*"[21]

According to the results of the Committee's Year 2000 survey only 25 per cent of government agencies had commenced Year 2000 compliance activities by June 1997.

In July 1997, the Minister for Information Technology and Multimedia requested Small Business Victoria to assume responsibility for informing the private sector of Year 2000 issues. The Committee was informed of a current lack of awareness of the Year 2000 problem among small to medium business enterprises (SMEs)[22] and is concerned at the implications of sector-wide business failures for Victoria's economy and the potential loss of vital government revenues.

In August 1997 the Minister for Information Technology and Multimedia wrote to all Ministers expressing concern that the Year 2000 issue was not receiving the level of attention required and requested details of each portfolio's Year 2000 action plans by 31 December 1997.

In December 1997 the Victorian Auditor-General's Office reviewed in detail the Year 2000 compliance activities of seven non-budget sector agencies in order to obtain a more in-depth view of their Year 2000 preparedness. In the May 1998 *Report on Ministerial Portfolios*, the Auditor-General reported that five of the agencies audited had not reached the stage of determining the work required to reach Year 2000 compliance.[23]

The Year 2000 action plans received by the Minister for Information Technology and Multimedia were reviewed by Arthur Andersen Consulting. Following Cabinet's consideration of the Arthur Andersen report[24] on the preparedness of the Victorian public sector, responsibility

[21] Victorian Auditor-General's Office *Report on Ministerial Portfolios*, May 1997, p.302
[22] Graeme Inchley, CEO, Y2K Industry Program, PAEC Private hearing, 12 August 1998
[23] *Report on Ministerial Portfolios*, Victorian Auditor-General's Office, May 1998, p.218
[24] The Arthur Andersen Report on the Year 2000-preparedness of public sector agencies was commissioned by the Minister for Information Technology and Multimedia in January 1998 and delivered in April 1998. The report is Cabinet in Confidence.

for centrally managing the risks associated with the Year 2000 problem was transferred to the Minister for Finance.

On 1 July 1998 the Minister for Finance established the Year 2000 Risk Management Unit, Department of Treasury and Finance, to monitor, report and verify the status of Year 2000 compliance of all budget sector agencies. From 31 August 1998 the Unit provided bi-monthly reports to Cabinet and from 30 November 1998 the Unit intends to provide monthly reports. Under these arrangements Cabinet Ministers have direct responsibility for the outcome of the government's Year 2000 risk management strategy for the public sector.[25]

(a) Policy Guidelines and Standards

The government's Year 2000 Policy was first issued in July 1996 and alerted CEOs and Department Secretaries to potential problems with processing date-sensitive data in the year 2000. The policy also contained model warranty clauses for inclusion in all IT acquisitions to reduce the government's exposure to the risks of the Year 2000 problem.

The government's policy for ensuring Year 2000 compliance in the private sector was initiated in July 1998 and is implemented by Small Business Victoria, Department of State Development, through the Minister for Industry, Science and Technology in conjunction with the Minister for Small Business.

(b) Annual Reporting Requirements

In July 1998 the Minister for Finance directed all departments and all agencies to include additional information on the Year 2000 problem in their 1997-98 annual reports. The new reporting requirements focus on data that can be used to assess the Year 2000 preparedness of individual agencies.[26]

The Committee understands that the accountability framework for annual reporting also allows an assessment of the risks of the Year 2000 problem to the whole of government, in terms of the status of "business critical services" such as the supply of potable water, revenue collection and medical equipment. These reporting requirements also include the Year

[25] PAEC Budget and Estimates hearing, The Hon. Roger Hallam, Minister for Finance, 27 July 1998, p.37 and Year 2000 Sub-Committee private hearing, Mr Adam Todhunter, Executive Director Year 2000 Risk Management Unit, 10 August 1998, p.6.

[26] Part 9 *Financial Management Act* 1994, "9.6 Year 2000 compliance requirements and disclosures"

2000 status of interconnected entities that interface and exchange date-sensitive data with agencies.

A copy of the *Year 2000 Annual Reporting Requirements* is at Appendix 8.

(c) Summary of Government Year 2000 initiatives

At an Estimates hearing the Minister responsible for managing the government's response to the Year 2000 issue, Hon. Roger Hallam, advised the Committee that the government had appointed a Ministerial Advisory Committee[27] consisting of senior officers from the Departments of Treasury and Finance, Premier and Cabinet, State Development, Justice, the Regulator-General, the Auditor-General and the Victorian Government Purchasing Board to advise on strategies to deal with the Year 2000 problem.

The Minister identified the main concerns as the need for contingency plans, the potential legal ramifications and the need for a coordinated approach to resolving the Year 2000 problem.

The Minister informed the Committee[28] that all business critical systems were expected to be compliant by 31 December 1998. The Minister also confirmed that the Year 2000 Risk Management Unit had received a commitment from the Premier for extra funds, if needed.

On 23 September 1998 the Minister for Industry, Science and Technology, Hon. Mark Birrell, launched the first of ten free information sessions on the Year 2000 problem specifically aimed at medium to small businesses. These information sessions involve a panel of experts with backgrounds in insurance, accounting and banking as well as representatives from businesses that have achieved Year 2000 compliance.

2.3 Commonwealth and international government activities

Two federal agencies have been given responsibility for ensuring that both public and private sectors are compliant by the Year 2000. The Office of Government Information Technology (OGIT) assists Federal Government departments in ensuring Year 2000 compliance for business critical systems while the Commonwealth Department of Industry, Science and Tourism assists small business.

[27] PAEC Estimates public hearing, The Hon. Roger Hallam, Minister for Finance, 27 July 1998, p. 37.
[28] *ibid*.

The 1998 Federal Budget allowed deductions for most costs relating to Year 2000 compliance[29] and announced legislation to provide immediate deductions for the costs of purchasing or re-engineering software before 1 January 2000. The legislation will also include tax concessions of 125 per cent for the costs of research and development associated with resolving Year 2000 problems.

The Federal Government initially allocated $127 million[30] to remedy specific Year 2000 problems in the Commonwealth public sector and to raise awareness about the Year 2000 problem in the Australian business community. The Year 2000 Project Office within OGIT administers these funds for technology-dependent Commonwealth agencies that deliver key services such as social welfare and unemployment payments, defence and national security, health and security and revenue collection. Commonwealth public sector agencies are expected to spend $600 million on addressing the Year 2000 problem.

The Year 2000 Project Office chairs and provides secretariat support to the Commonwealth/State Liaison Group. This group comprises Year 2000 Project Directors from all States, Territories and the Commonwealth and meets bi-monthly. Its objectives are:

- to understand and share information on how all levels of Australian government are addressing the Year 2000 problem;
- where possible, to identify the degree of readiness and cost to all levels of government;
- to identify mutual areas of concern to avoid duplication; and
- to identify where coordination is needed and where appropriate to identify specific areas of responsibility.

(a) Office of Government Information Technology

OGIT instigates third party auditing of Commonwealth agency compliance, provides advice on legal and compliance issues, establishes testing environments, deals with the needs of small agencies and raises awareness of current Year 2000 issues.

[29] Draft Taxation Ruling TR 98/D5, allows deductions for "expenditure on acquiring new software (including upgrades) or substantially rebuilding current software which has the predominant nature of ensuring Year 2000 compliance, provided that such expenditure is incurred up to 31 December 1999" cited from *The Australian Financial Review*, May 19 1998, p.35.

[30] The Hon John Fahey, MP, Minister for Finance and Administration and The Hon. John Moore, MP, Minister for Industry, Science and Tourism, joint media release, 15 April 1998; *The Australian Financial Review*, 15 April 1998, p.3.

Since December 1997 OGIT has provided quarterly reports on the Year 2000 compliance status of all Commonwealth agencies to the Federal Cabinet. OGIT has yet to make public the current compliance levels within government departments due to concerns regarding legal liability.

(b) Year 2000 National Steering Committee

The Commonwealth Department of Industry, Science and Tourism established the Year 2000 National Steering Committee in September 1997 to provide high level advice and to take a lead role in coordinating Commonwealth, State and industry initiatives.

The Steering Committee coordinates the 'Year 2000 National Strategy' for the private sector, raises awareness of the Year 2000 problem and encourages remedial and contingency planning action, particularly in relation to small and medium sized enterprises (SMEs).

Serious concerns have been raised by the Year 2000 National Steering Committee regarding misconceptions by SMEs about the nature and potential impact of the Year 2000 problem. A survey by the Australian Bankers Association in March 1998 found that many SMEs are overlooking the critical importance of their supply chain dependencies. As a result it has been suggested that 10 to 20 per cent of companies will collapse due to Year 2000 programs that have been poorly planned or poorly implemented.[31]

(c) International Council for Information Technology in Government Administration

To determine the progress of the Victorian public sector in addressing the Year 2000 problem against international benchmarks, the Committee referred to the Year 2000 Report by the International Council for Information Technology in Government Administration (ICA),[32] published in September 1997.

The ICA Report includes a description of the Year 2000 status of a number of developed countries including Australia as at August 1997.

The report contains the following general comments:

[31] Dr Adam Cobb (1998) communication with the executive of the Year 2000 National Steering Committee.

[32] Jensen, P. B. (1997) Guidelines and Recommendations on Year 2000 Issues: Report on Year 2000 Workshop Copenhagen, August 14 and 15, 1997. International Council for Information Technology in Government Administration {http://www.ogit.gov.au/ica/icay2k.htm}.

"The Year 2000 Workshop concluded that the problems related to the century dateshifts are significant and pervasive. Time is running out. Therefore there is an urgent need for top management attention in all parts of society. Government must take a lead as the problem affects all aspects of society. Inside the public sector, effort should be given to ensure (Year 2000 compliance) activities at all levels. Government should promote a broad understanding of the Year 2000 problem.

…The urgency of the issue was much emphasized. Many Information Technology (IT) Managers predict that their systems will fail before 2000 because they include processes for short term forecasting. December 31 1999 is not the target deadline, it is the absolute and final time by which all systems must be corrected, tested and implemented.

Top management responsibility implies that senior management must take charge of, and assume responsibility for, their organization's Year 2000 program. The breadth of issues dictates that it will be insufficient to attempt to drive the required process from a middle management perspective. Senior management holds the key to setting the agenda and the correct priorities for their organization.

Respective governments must take a lead role in addressing the Year 2000 date change issues, having an Overall Government Responsibility. The implications are far reaching and may affect all levels of society. In the public sector the prime objective is to ensure that the sector's ability to continue to provide services is not threatened. In regard to public utilities, governments must ensure awareness and require appropriate activity. Government must also take the lead in promoting awareness within the private sector.

The subject of embedded systems is a major cause of concern because of the general lack of information and this aspect requires special attention.

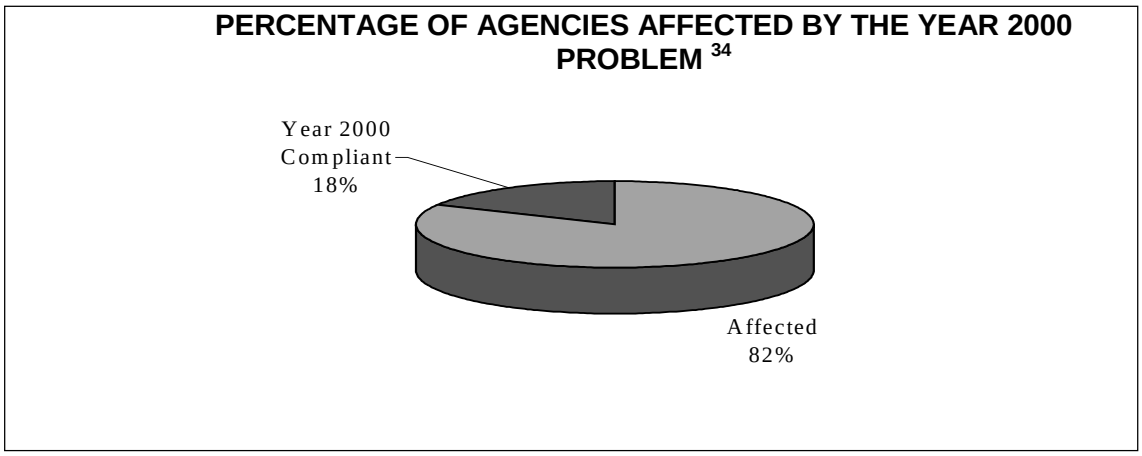
Year 2000 problems do not stop at the border of a country. No organization, committee, league or entity has taken responsibility for a worldwide view of problems and solutions. International relations and a well-coordinated approach are therefore needed. The relationship of the problems in advanced countries to less advanced countries has not been defined. The awareness issues should become the responsibility of the advanced countries.

The risk of introducing new major IT intensive projects, such as the European Economic and Monetary Union (EMU) related enhancements, in parallel with Year 2000 conversion, can create conflicting demands and this should be considered. Many public sector bodies have said that they intend to achieve Year 2000 compliance through the use of existing resources. This means that new IT applications and services cannot be developed and introduced if all existing resources are dedicated to the Year 2000 problem. The key point here is that it is widely recognized that IT resources are fully allocated to the Year 2000 problem and that skill shortages are likely to occur."[33]

2.4 Survey Results

Exhibit 3 shows the results of the Committee's Year 2000 survey for the proportion of public sector agencies (n=244) affected by the Year 2000 problem.

Exhibit 3



It shows that most public sector agencies (82 per cent) were affected by the Year 2000 problem at the time of the survey. The agencies that indicated they were Year 2000 compliant, are listed at Appendix 9.

Exhibit 4 shows the proportion of Year 2000 compliant agencies according to specific categories of public sector agencies.

[33] *Source*: P. B. Jensen, Leader of ICA Year 2000 Workshop and IT Manager, Ministry of Research and Information Technology, Copenhagen, Denmark, 26 September 1997.

[34] Survey data for the period 3 March 1998 to 31 July 1998.

Exhibit 4

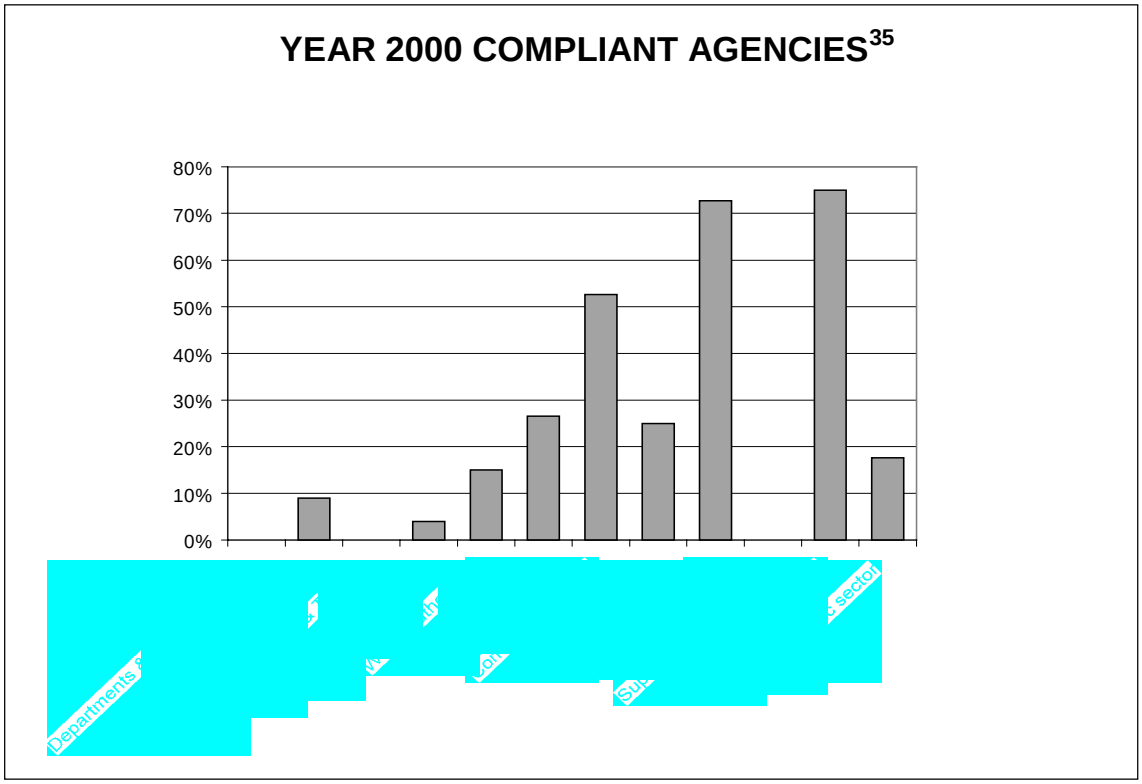


Exhibit 4 shows that most Year 2000 compliant agencies comprise public cemeteries, regional waste management groups and public companies, trusts and joint ventures. These small public sector agencies are less likely to be affected by the Year 2000 problem as they operate stand-alone desktop PCs and contemporary client server IT systems which have been updated or replaced with Year 2000 compliant systems. A further advantage for these agencies is that they do not have computer interfaces with third parties.

Public sector agencies such as government departments, universities and TAFE institutions and superannuation funds all have Year 2000 affected IT systems. Many of the larger government agencies operate legacy IT systems such as mainframe and mid-range computers that run in-house or third party applications. These legacy systems are likely to be affected by the Year 2000 problem. Furthermore, these agencies have a large exposure to computer interfaces with third parties such as banks, clients, government regulators and enforcement agencies, complicating their Year 2000 compliance requirements.

Exhibit 5 shows that most agencies affected by the Year 2000 problem had developed Year 2000 compliance plans.

[35] Survey data for the period 3 March 1998 to 31 July 1998. Note that the lack of columns for Departments, Universities and superannuation funds indicates that all of the respondent agencies within these categories were not compliant.

Exhibit 5

RESPONDENT AGENCIES WITH COMPLIANCE PLANS[36]

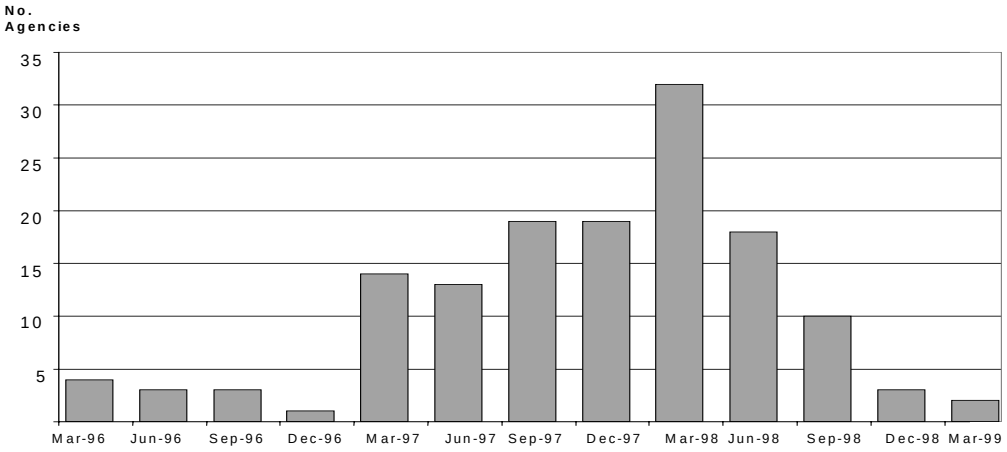
Public agency	No. agencies affected	No. with compliance plans	%
Departments & budget sector agencies	14	13	93
Public hospitals & ambulance services	72	54	75
Universities & other educational institutions	23	14	61
Municipal councils	48	30	63
Regional water authorities	16	8	50
Public bodies	47	35	74
Companies, trusts & joint ventures	10	10	100
Regional library corporations	6	1	17
Public cemeteries	3	2	67
Superannuation funds	4	3	75
Regional waste management groups	1	0	0
Total public sector	**244**	**170**	**71%**

Agencies which had not developed compliance plans include the small public sector agencies previously noted as mainly Year 2000 compliant. Survey responses indicated that some agencies did not need a compliance plan because their IT systems would be upgraded to compliant systems before 31 December 1999, as part of their normal business processes.

Exhibit 6 shows the survey results for the financial quarter in which public sector agencies commenced implementing Year 2000 compliance plans.

Exhibit 6

COMMENCEMENT OF COMPLIANCE PLAN (NUMBER PER QUARTER)[37]



[36] Survey data for the period 3 March 1998 to 31 July 1998.
[37] Survey data for the period 3 March 1998 to 31 July 1998.

Exhibit 6 shows that most agencies commenced Year 2000 compliance activities in late 1997 to mid-1998. The Committee accepts that agencies may have been assessing their exposure and developing compliance plans in the intervening period. However, the Committee is greatly concerned that some agencies do not plan to initiate Year 2000 compliance programs until late 1998 or early 1999. The Committee stresses the maxim, the earlier the better with an emphasis on starting **now.**

The Committee recommends that:

Recommendation 2.1:	***To expedite corrective efforts, those agencies which have not commenced compliance projects, be directed by the government to commence immediately and to publish details of the commencement dates in the report to the Parliament on the Year 2000 problem in the autumn session of 1999.***

2.5 The scope of the problem

One difficulty in assessing risk exposure is determining the scope and nature of the problem. Year 2000 failure may occur in software and hardware, it may occur in equipment that is not obviously date reliant and in areas of operation that are far removed from IT systems.

One of the major difficulties in dealing with the Year 2000 problem is simply recognising the potential for its existence and what, in practical terms, may be the consequences of its occurrence. For example, one of the world's first legal cases relating to the Year 2000 problem was against a company which manufactured a non-compliant cash register system that would not process debit/credit cards with expiry dates in 2000 or later.[38] A grocery store successfully sued the company for the loss of business relating to its inability to process debit/credit cards.

The Committee believes that the issue has been trivialised by media campaigns which depict the Year 2000 problem as a "bug" that can be simply "stepped on". The issue is also described as an "IT" problem which, as for many programming errors or computer viruses, can be quickly remedied by a software patch. The Committee has found that this is simply not correct and believes it is important that a broad-based education and awareness program, aimed at alerting management to the scope of the Year

[38] Reported in *The Age*, 22 September , 1998, *IT2* p.4

2000 problem, be undertaken as soon as possible. The focus should be on the need for a wide, whole of business review and the development of contingency plans. The campaign should use plain language and avoid use of the term "bug" or images of insects.

The Committee believes that the initial lack of appreciation of the significance of the Year 2000 problem resulted in a slow response by the government and agencies. Consequently the level of awareness of the potential ramifications of the Year 2000 problem in the wider Victorian community has also been low. Strong community leaders will be needed to prepare and organise the necessary community contingency plans for the potential consequences of the Year 2000 problem. The preparation of the community for the Year 2000 problem should be one of the government's highest priorities for 1999.

The Committee recommends that:

Recommendations 2.2:	***The government develop and implement a new public awareness campaign for the public sector and the community clearly outlining what the Year 2000 problem is, the consequences of non-compliance, what aspects of service or business operations it may affect, sources of information and assistance and stressing the need for immediate action.***

Recommendation 2.3:	***An objective of the campaign be raising awareness of the various levels of risk for business continuity.***

Recommendation 2.4:	***The campaign be aimed at educating a wide audience of the need for contingency planning.***

Recommendation 2.5:	***The awareness campaign be in plain language and avoid the use of terms or images that depict a "bug".***

2.6 Ownership of the Year 2000 problem

Currently the Year 2000 problem has a relatively low profile in the community. However, the Committee expects that the problem will become

a major issue in the months leading up to the year 2000, especially if date-related failures progressively occur in 1999.

The Committee believes that it is appropriate for the government to provide leadership on this issue and to demonstrate to the community that strategies are in place to ensure minimum disruption of services.

The Committee recommends that:

Recommendation 2.6:	***The Department of State Development liaise with peak industry bodies and organise industry forums to facilitate the sharing of information on common problems and solutions. These industry groups should be involved in identifying critical problems and assist in developing industry-wide contingency plans.***

Recommendation 2.7:	***Greater awareness be made of the problems that can occur due to the interconnectivity of business systems and the probable manifestations of the Year 2000 problem that will occur in all date-dependant embedded chip technology.***

Recommendation 2.8:	***Agencies distribute information, on a regular basis, to staff and customers in order to build commitment and to communicate progress on Year 2000 compliance.***

Recommendation 2.9:	***There is sharing of information on best practice for dealing with the Year 2000 problem amongst public sector agencies and between public and private sectors.***

2.7 Summary

The government's Year 2000 Policy was originally based on a level of awareness that was prevalent in the IT community at the time of its introduction. In July 1996 the Year 2000 problem was regarded as an IT management issue rather than as a business continuity or risk management issue. The lack of awareness of the dimensions of the Year 2000 problem

has been a factor which initially delayed the timely initiation of Year 2000 compliance activities across the Victorian public sector.

The government's direction that all funds for correcting the Year 2000 problem were to be made available from internal budgets may also have given Chief Executive Officers the wrong message in terms of the scope of the problem, the level of urgency and high priority required.

Since July 1998, the government has commenced addressing the Year 2000 problem on a whole of government risk management basis, supported by central reporting to Cabinet and the allocation of additional funds.

Chapter 3:The Risks Associated with the Year 2000 Problem

> *"I think that's bought a realisation that no matter how much work you do, you can never be absolutely sure that there isn't some little device stuck in the bottom of the power station somewhere"* [39]

3.1 Possible consequences

The Year 2000 problem is recognised worldwide as a major risk to both the public and private sectors. Due to the interdependencies of businesses for the production and supply of goods and services, the problem may extend to entire sectors of the Victorian economy.

The impact of date-sensitive computer programming errors on business continuity are already known. For example, due to a Year 2000-related problem:

- on December 30, 1996 computers which control the production of aluminum shut down smelter operations in New Zealand, Tasmania and South Australia because they were not programmed to recognise the 366th day of the leap year;
- in 1997 the stock exchange in Brussels shut down for two hours causing lost revenues of $A1 million;
- on the 29 February 1996, a US lottery company could not make any payouts because the system did not recognise the additional day for February;
- Visa International credit cards issued with expiry dates of "00" could not be processed by automatic teller machines, cash registers or electronic funds transfers at point of sale systems;[40]
- some hospital appointment systems in the UK have failed to record patient appointments made for the year 2000; and
- some pharmacy supply companies are unable to extend batch expiry dates beyond 1999 and Computed Tomography (CT) scanners have locked up when tested for year 2000 operation.

The Year 2000 problem is therefore pervasive and its impact is potentially severe and unpredictable.

[39] Mr Theo Van Der Meulen, SMS Consulting Group Pty. Ltd., PAEC Private hearing, 10 September 1998.

[40] The first legal case relating to the Year 2000 problem was against a company that manufactured non-compliant cash registers that would not process credit cards with the "00" expiry date. The US case was settled out of court in September 1998. *The Age*, 22 September 1998, *IT2* p.4.

3.2 What risks does the Victorian public sector face?

Public sector agencies deliver vital services to the community. These include hospital care, water supply, gas, police, emergency and rescue services and transport systems. Ultimately, too, the government is responsible for the delivery of electricity. These services use date-sensitive systems to perform a variety of business processes and to control and monitor the operation of critical plant and equipment.

If such systems fail the consequences for the community may be serious and widespread, unless there are effective contingency plans in place.

Embedded chip technology has the potential to impact on the essential infrastructure systems that underpin Victoria's economic system such as the electricity supply, water and sewerage treatment, gas supplies and telecommunications systems. Non-compliant embedded chips are far harder to detect due to their vast numbers.[41]

3.3 Strategies to reduce risk

Based on responses from agencies, the following general observations can be made:

- the Victorian public sector has a number of in-house developed older (legacy) systems which are more prone to the Year 2000 problem. Modification or replacement strategies may be required;
- during the last couple of years there has been a trend to the use of package software. In these circumstances an upgrade or replacement strategy is more likely than a modification strategy for Year 2000 compliance; and
- the high number of personal computers suggests that there may be a high degree of end user computing. Therefore users may have modified applications in such a way as to render them business critical and subject to Year 2000 problems. In these circumstances modification or replacement strategies may be needed.

Based on the results of the survey for the period March to July 1998:

- thirty per cent of respondent agencies had high risk exposure due to the use of legacy systems and applications;
- thirty per cent of respondent agencies had medium exposure due to the use of business critical data systems or applications on PCs;

[41] PAEC private hearing, 10 September 1998, Mr Theo Van Der Meulen, SMS Consulting Pty Ltd., p.4.

- ten per cent of respondent agencies had low exposure due to the achievement of compliance; and
- thirty per cent of respondent agencies, did not respond to the question and therefore have an unknown risk exposure.

As previously outlined, the government has adopted a position whereby each agency is responsible for ensuring business continuity through the year 2000 transition period and for managing the business management risks of the Year 2000 problem. A central reporting framework, reporting to Cabinet, to allow Government oversight of the response of the public sector recently augmented this approach.

However, while the Committee welcomes this initiative, it is concerned that resources across the public sector may not be centrally coordinated to ensure that they are directed to areas of highest risk and therefore most urgent need. For example, some agencies have contracted external consultants to address the Year 2000 problem while other agencies with relatively more important services face a shortage of appropriately qualified computer technicians, inadequate funds and have not prepared Year 2000 compliance plans.[42]

The Committee believes it is essential that a whole of government approach continues to be adopted for assessing the risks of the Year 2000 problem to the operations of government and to the community. This approach will ensure that critical systems such as electricity, water, gas, emergency services, hospitals, transport and telecommunications receive the necessary support to meet compliance. As a matter of urgency, the government should prioritise and rank all business critical systems from a whole of government perspective, on the basis of risk to the community and direct resources to the identified priority areas.

3.4 What the Committee found

Exhibit 7 shows the percentage of agencies' compliance plans that address the various risk exposures.

[42]For example, survey responses for the Austin and Repatriation Medical Centre and St. Vincent's Hospital indicate a shortage of in-house IT resources.

Exhibit 7

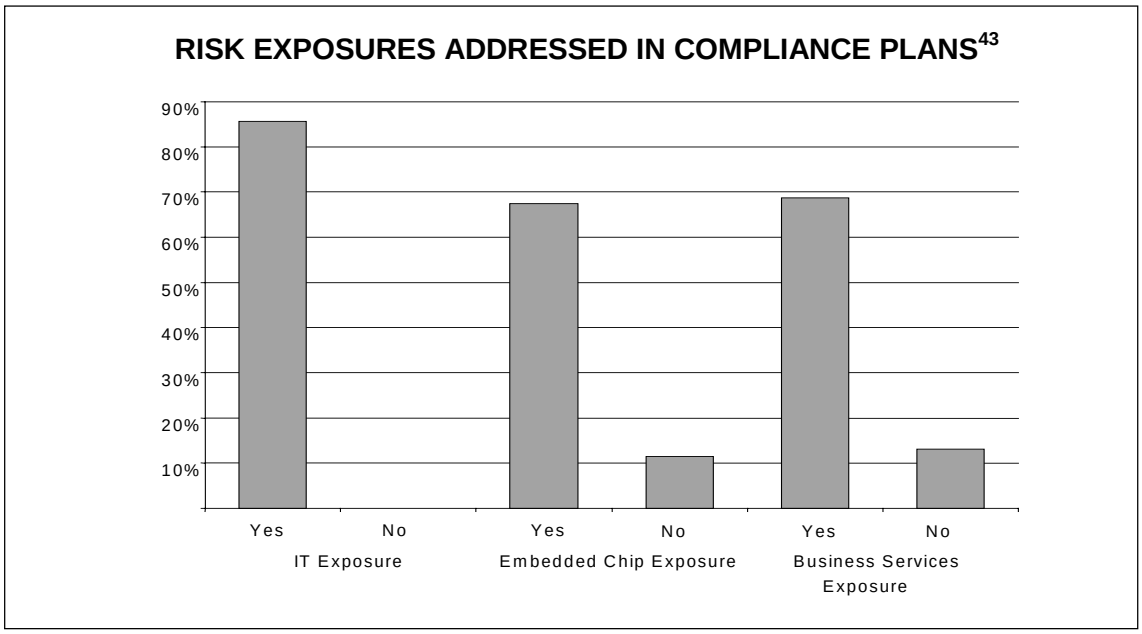


Exhibit 7 shows that the majority of public sector agencies that responded are addressing the risks of the Year 2000 problem for IT systems, embedded systems and business services.

Although agencies may have addressed all internal Year 2000 compliance issues some may be exposed to the possible failure of external parties who may themselves experience business continuity problems. Such failures may cause interruptions to the delivery of goods and services creating the potential for business failure and litigation arising from the failure to supply.

Although 86 per cent of respondent agencies had compiled inventories of the risk exposure of their IT systems, 32 per cent had not accounted for the risks posed by embedded systems or business services. Some of the crucial risks identified in embedded systems and business services include:

- the failure of medical equipment such as blood gas analysers, cardiac defibrillators, control monitors, kidney dialysis and ultrasound machines, ventilators or infusion pumps;
- office building closures for health and safety reasons;
- loss or malfunction of security and emergency warning systems;
- loss of food supplies, linen services, pathology and radiology or medical and pharmacy supplies for hospitals;

[43] Survey data for the period 3 March 1998 to 31 July 1998.

- loss of supply chains that support ongoing business requirements such as office supplies, spare parts, maintenance services;
- failure of PABX systems and internal business telecommunications systems;
- shut down of air-conditioning systems and other building control systems such as lifts and elevators; and
- computer failures due to loss of automatic cooling systems (HVACS) or the failure of uninterruptible power supply (UPS) systems.

The Committee was concerned that agencies focusing on business critical systems such as pay roll and financial management systems may fail to address other less obvious yet still business critical computerised systems. For example, systems for monitoring the operation of plant and equipment, internal telecommunications (e.g. PABX), building environmental controls (e.g. air conditioning, heating and cooling systems) and security and safety warning systems (e g. fire and security access systems). Agencies must also consider the need to include alternative supplies of water, gas or electricity in their contingency plans.

The survey results revealed that public hospitals, metropolitan and regional water authorities, ambulances, emergency services and local councils had not commenced to compile an inventory of their embedded systems. Although Victoria Police has completed an inventory of all the potentially affected embedded systems across its organisation, it had not allocated any funds or priorities for their remediation.[44]

3.5 Dealing with external parties

Many agencies have computer systems which interface and exchange date-sensitive data with external parties in both the public and private sectors. Victoria Police and VicRoads may exchange date-sensitive data (e.g. to administer the demerit points system or motor vehicle licensing) and the Department of Justice may exchange date-sensitive data (e.g. court schedules, criminal sentences, prison custody or parole records) with a number of authorities in relation to the administration of the criminal justice system.

[44] Survey data for the period 3 March 1998 to 31 July 1998.

External relationships identified by agencies include:

- trading suppliers of goods and services including contractors undertaking pay roll, companies with electronic commerce/data interchange systems;
- specialised IT service providers for the hospital casemix payment system;
- commercial businesses such as banks, investment management services, central supply panel contractors for fuel and electricity; and
- clients including the motor vehicle registry, police, government regulators.

The Committee stresses that the risks presented by interfacing computers need to be taken into consideration during an agency's Year 2000 planning phase to ensure that all external parties are consulted and cooperate to ensure mutual Year 2000 compliance.

Exhibit 8 shows between 18 per cent to 50 per cent of respondent agencies have included the potential risks relating to external parties in their compliance plans. The figures in this Exhibit reflect the types of external parties that will be consulted by agencies, rather than the adequacy or the level of consultation needed.

Exhibit 8

COMPLIANCE PLANS INCLUDING EXTERNAL PARTIES[45]

Public agency	*No. agencies affected*	*Customers*	*%*	*Banks & financial institutions*	*%*	*Government & regulatory agencies*	*%*	*Electronic Data Interchange*	*%*	*Other*	*%*
Departments	14	10	71	6	43	12	86	5	36	1	7
Public hospitals	72	9	13	16	22	42	58	11	15	16	22
Universities & TAFEs	23	6	26	5	22	9	39	2	9	3	13
Municipal councils	48	14	29	23	48	16	33	7	15	8	17
Water authorities	16	3	19	6	38	7	44	5	31	1	6
Public bodies	47	18	38	15	32	24	51	4	9	9	19
Companies, trusts	10	3	30	6	60	6	60	2	20	2	20
Regional libraries	6		0		0	4	67	1	17	4	67
Public cemeteries	3		0	1	33	0	0		0	1	33
Superannuation funds	4	1	25	4	100	2	50	2	50		0
Waste management	1		0		0		0		0		0
Total public sector	**244**	**64**	**26%**	**82**	**34%**	**122**	**50%**	**39**	**16%**	**45**	**18%**

[45] Survey data for the period 3 March 1998 to 31 July 1998.

Comments on the survey form and evidence taken by the Committee indicate that this task has not been completed, and some agencies may not be considering their exposure as widely as they should.

The Committee recommends that:

Recommendation 3.1:	***The Year 2000 Risk Management Unit assess the need for further compliance work in public sector agencies which have yet to account for the potential effects of the Year 2000 problem on business continuity and service quality.***

The Committee was advised[46] that some agencies are approaching suppliers and other external parties for warranties or other forms of written assurance. A warranty places an obligation on the supplier, gives some confidence that the product will perform as intended and provides the basis for compensation should the product fail. However, a warranty does not protect against failure itself, or against the effects of failure on the business.

The Committee understands that most external parties are reluctant to provide any written assurances because of potential legal action. Instead they are giving government agencies letters of comfort without any specific guarantees that they will supply fully compliant IT products or services.[47]

The Committee is also aware that there is a current need for the coordination of standards for data interchange across the whole of government and between the public and private sectors. The establishment of interchange standards needs to be a priority if the Year 2000 data interface problem is to be resolved before 31 December 1998.

The Committee recommends that:

Recommendation 3.2:	***Priority be given to the development of interchange standards if the Year 2000 data interface problem is to be resolved before 31 December 1999.***

[46] For example, PAEC private hearings 28 August 1998, 10 and 11 September 1998.
[47] For example, PAEC private hearing, 28 August 1998, pp.4-5 and 10 September 1998, (SMS Consulting Group Pty Ltd., p.10).

The Committee believes that it is essential that every agency ensure that it will not be affected by the failure of business critical systems on which it relies. This highlights the need for compliance plans of agencies to incorporate a program of testing to provide proper assurance that systems will work as intended. This is further discussed in Chapter 6 "*Implementation, Management and Monitoring Strategies*".

3.6 Contingency plans

The Committee recognises that certain areas of an agency's operation may not be remediated prior to critical dates. To avoid disruptions from the failure of business critical systems, agencies must develop manual alternatives to automated tasks. This may involve:

- the need to consider, plan and implement a manual alternative. This may require the hiring and training of human resources to perform vital tasks and to create a back up system and the reactivation of manual systems; and
- if the potential failure is in a business critical area, the development of a disaster recovery plan.

This is particularly important where there is a foreseeable risk, such as personal injury or other consequential damage, if equipment or a system malfunctions or ceases to operate.

The extent of the impacts of the Year 2000 problem are indeterminate, however, given the significant funds and resources directed at resolving non-compliant systems in 1998-99, the Committee believes that the risks will be minimal. Given that the Year 2000 problem may have systemic, progressive and possibly compounding effects in 1999 and throughout 2000, there is a need for all agencies, businesses and the community to prepare contingency plans.

Contingency plans must be formulated to enable businesses to continue to operate independently of their business critical IT systems or embedded technology devices. For example, if a business uses a just-in-time ordering system that is dependent on a computerised stock taking system, it should stock extra quantities of goods to allow the business to continue to operate through any supply disruptions in 2000.

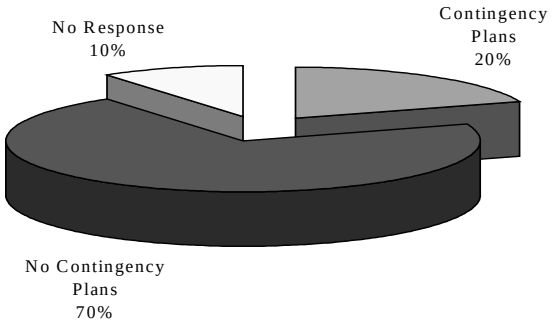
The Committee notes that for critical businesses such as the electricity supply industry, which is dependent on the continuity of their IT systems and embedded technology, contingency planning will help minimise the duration of potential outages. Such utilities should ensure that their emergency response teams are given additional personnel or personnel

trained to cope with the Year 2000 problem, extra resources, materials and equipment in preparation for potential service failures in 2000.

Exhibit 9 shows the percentage of respondent agencies in the Victorian public sector with contingency plans.

Exhibit 9

AGENCIES WITH CONTINGENCY PLANS[48]



At the time of the survey most agencies did not have contingency plans prepared for the Year 2000 problem.

Exhibit 10 shows further detail of the types of agencies and their situation concerning contingency plans.

Exhibit 10

AGENCY CONTINGENCY PLANS[49]

Public agency	***No. agencies affected***	***No. with contingency plans***	***%***	***No. without contingency plans***	***%***
Departments & budget sector agencies	14	5	36	8	57
Public hospitals & ambulance services	72	13	18	55	76
Universities & TAFEs	23	9	39	14	61
Municipal councils	48	6	13	38	79
Regional water authorities	16	3	19	11	69
Public bodies	47	9	19	32	68
Companies, trusts & joint ventures	10	3	30	3	30
Regional library corporations	6		0	4	67
Public cemeteries	3	0	0	3	100
Superannuation funds	4	0	0	4	100
Regional waste management groups	1	0	0		0
Total public sector	**244**	**48**	**20%**	**172**	**70%**

[48] Survey data for the period 3 March 1998 to 31 July 1998.
[49] Survey data for the period 3 March 1998 to 31 July 1998.

Exhibit 10 shows that the majority of hospitals and ambulance services, municipal councils and regional water authorities had not developed contingency plans for the Year 2000 problem. It is crucial that these agencies continue to provide their services in 2000 without major interruptions. The Committee believes that contingency plans should be developed for **all** business critical areas, as it is inevitable that some unknown and unforeseen risks will occur in 2000. The Committee makes a number of recommendations aimed at improving the present state of readiness of the public agencies for the Year 2000.

The government needs to focus on central risk assessment to ensure the delivery of essential services and provide greater support for contingency planning in agencies that may fall behind in their Year 2000 projects.

The Committee recommends that:

Recommendation 3.3:	***The government determine whole of government priorities for remediating business critical systems based on such criteria as the potential for adverse health and safety effects, adverse financial effects on the community, detrimental effects on security and adverse economic consequences.***

Recommendation 3.4:	***The government assess the State's Year 2000 risks, including those posed by key economic sectors.***

Recommendation 3.5:	***The Year 2000 Risk Management Unit build and maintain close links with the essential infrastructure organisations in order to be aware of the status of Year 2000 compliance programs.***

Recommendation 3.6:	***Businesses and departments be encouraged to identify areas where a manual backup should be considered as part of their contingency planning.***

The Committee recommends that *(continued)*:

Recommendation 3.7:	***To ensure that risks are minimised in the interests of patient safety, the Department of Human Services assess the readiness of public and private hospitals and medical facilities for the Year 2000 problem.***

Recommendation 3.8:	***The Office of the Regulator-General assess and report to Parliament on the Year 2000 readiness of all electricity generation and distribution units and the potential impact of the Year 2000 problem on the transmission system.***

Recommendation 3.9:	***The Bureau of Emergency Services Telecommunications assess the impact of the Year 2000 problem on the emergency response systems that are dependent on the Global Positioning System satellite system and emergency radio, microwave communications systems and computer aided call and dispatch systems.***

Recommendation 3.10:	***The Police and the Country Fire Authority and the Metropolitan Fire and Emergency Services Board undertake an awareness campaign so that property owners have all security and fire alarms Year 2000 compliant by July 1999.***

Recommendation 3.11:	***The Department of Natural Resources and Environment assess the readiness of all water authorities and waste water treatment facilities for the Year 2000 problem. The Department make known problems and potential solutions for specific vendor-supplied systems and equipment.***

The Committee recommends that *(continued)*:

Recommendation 3.12:	***That the Victorian WorkCover Authority, in light of its responsibilities under the Occupational Health and Safety Act 1985 and the Dangerous Goods Act 1985, seek assurances from all licensees that they will be Year 2000 compliant, follow up and assess those responses and report to the Parliament on this matter in autumn 1999.***

Recommendation 3.13:	***The Office of Corrections assess the impact of the Year 2000 problem on security and environmental control systems in prisons.***

Chapter 4:The Cost of Achieving Year 2000 Compliance

> *"The cost of Year 2000 is the cost of staying in business: we intend to stay in business"* [50]

4.1 Introduction

The cost of achieving Year 2000 compliance across the public sector will be extremely high as it will entail the commitment of considerable human and financial resources,[51] replacing computer hardware or software, or all three solutions in various combinations. The other cost consideration involves investigating, identifying, fixing and testing embedded chip technology – this is likely to be a very expensive undertaking. For example, consultants[52] have estimated that Australia's listed property owners will need to spend $20 million to address Year 2000 problems in lifts, air conditioning, security and fire services in their office buildings.

The Gartner Group,[53] a market research firm, estimates the total global cost of remediation to be more than $A965 billion with a substantial part of the expenditure to be made in 1999. The United States of America has estimated the cost of remediation for public agencies at $A10.7 billion.[54] .The total estimated cost of correcting the Year 2000 problem in Australia for both the public and private sectors, is estimated to be at least $A11 billion.[55] According to company statements to the Australian Stock Exchange, the top 150 Australian companies have estimated their costs at $4 billion.[56] Telstra has estimated its Year 2000 costs at $500 million and a survey undertaken by the Reserve Bank of Australia has revealed that the Australian banking sector has earmarked $600 million for Year 2000 compliance spending. A list of government and private sector company costs is provided at Appendix 10.

---

[50] Ms. Negba Weiss-Dolev, Group Director, Year 2000 Programme, Telstra, responding to a question about the size of Telstra's budget to address the Year 2000 problem. PAEC Private hearing, 11 September 1998.

[51] A large reprogramming project of 40 million lines of code would typically take 9 months to one year to complete the planning phase using approximately 20 personnel, depending upon the diversity of the computer systems in use.

[52] Merrill Lynch research consultants, in The *Australian Financial Review*, 24 August 1998, p.32.

[53] *The Australian*, 14 October 1998, p.58

[54] *The Age*, 15 September 1998

[55] From various reports in the media previously cited in Chapter 1.

[56] *The Australian*, 21 September 1998, based on estimates by consultants Deloitte Touche Tohmatsu *http://www.deloitte.com.au/*

The Commonwealth Minister with responsibility for the Year 2000 problem, Hon. John Fahey, estimates the cost of correcting Commonwealth Government business critical systems is $600 million.[57] The Office of Government Information Technology (OGIT) advised that the Commonwealth Government provided $120 million in April 1998 and officials indicated that this additional seed funding gave much needed impetus to the public sector's Year 2000 compliance program.[58]The Committee was advised that up to that point much of the $600 million dollars required by Commonwealth agencies was to be funded through internal cost arrangements.

The Committee is aware that a substantial proportion of the cost of replacing hardware and upgrading software may be treated as normal or accelerated asset replacement by agencies.

4.2 Year 2000 survey results

Exhibit 11 shows that at the time of the survey[59] only 67 per cent of agencies had identified the costs directly attributed to their remediation program.

The remaining agencies were unable to provide an estimate of past or future costs because:

- Year 2000 compliance was part of their normal IT upgrade process and the costs were not separately recorded;
- some had not fully assessed the extent of the problem and so were unable to estimate the amount of work to be undertaken; and
- the estimates provided were often very broad and would change according to the solutions chosen.

[57] Hon. John Fahey, Minister for Finance and Administration, Press Release, 24 April 1998
[58] PAEC Private hearing, 12 August 1998.
[59] Survey data for the period 3 March 1998 to 31 July 1998

Exhibit 11

COST OF ACHIEVING YEAR 2000 COMPLIANCE IN THE VICTORIAN PUBLIC SECTOR[60]

Public agency	*No.affected agencies responding (%)*	*Costs incurred ($)*	*Total estimated costs ($)*	*Proportion expended (%)*
Departments, budget sector agencies [(a)]	86	7,775,000	116,350,000	5
Public hospitals & ambulance services[(b)]	79	7,371,450	107,500,000	7
Universities & educational institutions	74	5,472,000	13,134,400	42
Municipal councils [(c)]	48	2,421,604	24,697,800	10
Regional water authorities	82	503,000	5,598,000	9
Public bodies [(d)]	55	15,229,105	62,846,400	56
Companies, trusts & joint ventures	78	3,568,000	9,490,000	38
Regional library corporations	50	3,300	40,000	8
Public cemeteries	67	-	234,000	0
Superannuation funds	50	-	290,000	0
Regional waste management groups	100	4,000	4,000	100
Total public sector	**67**	**42,347,459**	**340,184,600**	**12%**

Notes:

(a) The Department of Human Services estimate of $95 million was reduced to $45 million following evidence presented to the Committee.[61]

(b) The survey result for hospitals and ambulance services was $46 million. The Department of Human Services Year 2000 program for public hospitals and ambulance services estimates $107.5 million.[62]

(c) The survey result for councils was $18.5 million, this has been updated to $24.7 million to accord with survey material presented to the Committee by the Deputy Secretary for Local Government, Planning and Market Information Services Division, Department of Infrastructure, PAEC Private hearing, 10 September 1998.

(d) The Public Bodies estimate of $27.3 million was increased by $35.5 million following further information provided by the Public Transport Corporation ($20 million) and VicRoads (in excess of $15.5 million).[63]

The costs where IT systems have been, or will be, upgraded to Year 2000 compliant versions as part of an agency's normal IT replacement program were not included in the above results.

[60] Survey data for the period 3 March 1998 to 31 July 1998

[61] Evidence presented at PAEC Private hearing, 10 September 1998

[62] Evidence presented at PAEC Private hearing, 10 September 1998

[63] Evidence presented at PAEC Private hearings, 28 August 1998 (VicRoads) and 11 September 1998 (Public Transport Corporation)

In response to the Committee's Year 2000 questionnaire the total cost estimated by two-thirds of Victoria's public sector agencies is approximately $340 million.

As can be seen from the above Exhibit, the costs of addressing the Year 2000 problem at an agency level are high. Only 12 per cent of the total estimated cost had been expended as at 30 June 1998.

Most of the $340 million needed or planned by agencies for Year 2000 compliance projects is expected to be expended in 1998-99.

The Victorian Government has adopted a similar policy to Commonwealth Departments, where public sector agencies are expected to fund their respective Year 2000 compliance programs from their current global budgets. In Victoria extra funds will be committed as required and deemed necessary by the government.

The only other specific additional funding commitments that the Committee is aware of are:

- an extra $1 million for the replacement of some biomedical equipment in public hospitals;
- an annual allocation of $1.25 million for Year 2000 Project Coordinators in metropolitan and rural hospitals; and
- an annual budget of $600,000 for the Year 2000 Risk Management Unit.

A number of agencies indicated in their response to the questionnaire that lack of resources and specific funding were hampering progress with achieving compliance. This situation particularly applied to hospitals, councils and Victorian Police. Victoria Police indicated in May 1998 that they would require $30 million. Its budget for 1998-99 was subsequently shown as $1.5 million.[64] The Committee understands that some additional funding has now been provided but this will not be sufficient to ensure that all critical systems will be compliant. The Committee was encouraged by the Minister for Finance's assurance that the Government would commit additional funds where required.

The Committee noted that the agencies making the most progress to date are public bodies, Universities and TAFEs, Companies, Trusts and Joint Ventures and Regional Waste Management Groups, which have independent funding. Most of these agencies have relatively new IT

[64] Figures provided in survey response received in May 1998 and at PAEC Private hearing, 10 September 1998.

equipment, and few IT in-house legacy systems. In contrast, most inner budget agencies, hospitals, municipal councils, regional water authorities and superannuation funds which service a much wider customer base have made only limited progress in achieving Year 2000 compliance. Of these agencies, hospitals and water authorities present high risks to public health and safety and should be high priority in any additional financial allocations for Year 2000 remediation.

Within the inner budget, the Department of Justice, with responsibility for the police, the criminal justice system, Office of Corrections and emergency services also presents a high risk given the levels of expenditure on Year 2000 still needed.[65] The government will need to consider providing additional funding to those agencies which have a high dependence on technology and have a high level of risk if their systems are not compliant.

Exhibit 12 indicates progress made by agencies in terms of their expenditure profiles:

Exhibit 12

PREPAREDNESS OF PUBLIC SECTOR AGENCIES[66]

Public Agency	*No. agencies affected*	*No. agencies with Nil expenditure to date*	*%*	*No. agencies with unknown Year 2000 costs*	*%*
Departments & budget sector agencies	14	1	7	2	14
Public hospitals & ambulance services	72	34	47	20	28
Universities & TAFE institutions	23	10	43	7	30
Municipal councils	48	17	35	14	29
Regional water authorities	16	7	44	4	25
Public bodies	47	6	13	12	26
Companies, trusts & joint ventures	10	2	20	1	10
Regional library corporations	6	2	33	3	50
Public cemeteries	3	3	100	1	33
Superannuation funds	4	3	75	2	50
Regional waste management groups	1				
Total public sector	**244**	**85**	**35%**	**66**	**27%**

[65] The survey return for the Department of Justice indicates as expenditure of $500,000 from a total budget of $4.3 million.

[66] Survey data for the period 3 March 1998 to 31 July 1998

The Committee is concerned that at the time of the survey:

- almost half of all public hospitals had not commenced planning for Year 2000 compliance and nearly a third had not estimated the cost of addressing the Year 2000 problem;
- a third of municipal councils had not undertaken any steps to address the Year 2000 problem; and
- a very high proportion of superannuation funds had not made any progress on the Year 2000 problem.

The cost implications of ensuring Year 2000 compliance will become more pressing once each agency has clearly identified the extent of risk and the necessary remedial actions needed.

The Committee understands that over half of the agencies (56 per cent) that have formed task forces are using contractors to deal with the Year 2000 problem. The Committee was advised that skilled consultants with Year 2000 experience are in high demand, and as the year 2000 approaches, will be more costly to buy in - even assuming that they are available at the time. The Committee believes that these factors should provide a strong incentive for agencies to complete their compliance plans as soon as possible.

The costs involved and the limited skilled resources available to address this problem also highlight the important role that the Year 2000 Risk Management Unit plays in facilitating the exchange of information between agencies in solving common problems.

The majority of respondent agencies broadly indicated that they need to address their Year 2000 problem. Unless additional funding and resources are readily available, the possibility exists that core functions of government could be adversely affected.

The Committee believes that where high priority Year 2000 projects are dependent on additional funding, as is the case with hospitals and police, funds should be made available immediately. The time lag for agencies with business critical systems places unacceptable pressure on the ability of agencies to correct, test and achieve year 2000 compliant systems within an acceptable timeframe.

The Committee recommends that:

Recommendation 4.1:	***The government make it more widely known, particularly to SMEs, that the cost of the Year 2000 problem represents the cost of staying in business.***

Recommendation 4.2:	***The government allocate priorities across all agencies for Year 2000 funding commitments according to a risk assessment undertaken by the Year 2000 Risk Management Unit.***

Recommendation 4.3:	***In the event that key agencies are unable to meet the cost of compliance for business critical systems from within their budget, the government allocate the required funding.***

Recommendation 4.4:	***As a means of monitoring the achievement of Year 2000 compliance, the government track agencies' expenditure against year 2000 compliance plans.***

Recommendation 4.5:	***Agencies' annual reports include information on their total year 2000 expenditure and the sources of all internal and external (i.e. Advance to the Treasurer) funds.***

Chapter 5: Adequacy of Planning for the Year 2000 problem

> *"Until recently this task was being driven by IT managers who sit in middle level structures in Departments and this is not an IT issue, it's a business management issue of the highest order."* [67]

5.1 International best practice

The International Council for Information Technology in Government Administration (ICA) described best practice as the completion of all corrective action and the testing of changed systems by the end of 1998.

Further characteristics identified by the ICA of agencies that have achieved best practice in Year 2000 compliance, include:

- a full inventory completed prior to January 1997;
- Year 2000 status effectively communicated both internally and externally;
- at least 50 per cent of IT remediation completed and system testing strategy defined and started by February 1998;
- a senior director is made responsible for project management and the budget allocated; and
- expansion of the agencies' compliance program into industry, suppliers, clients and talking to other stakeholders as well as competitors.

Best practice also includes the development of contingency and disaster recovery measures to protect the most significant business processes should agencies fail to convert these systems on time. Every business critical function that relies on a computer system should have a contingency plan. These should have been developed in 1997, be tested and in place by 31 December 1998.

The greatest amount of effort will be required for testing, to ensure that the date processing changes have not introduced new errors into stable systems.

The US Federal Financial Institutions Examination Council in May 1997 set the following policies and guidelines for US banks:

[67] Mr Mike Harrington, Director, Special Projects Unit, Department of Premier and Cabinet, PAEC private hearing, 11 May 1998, p.1.

- complete inventory of core computer functions and set priorities for Year 2000 goals by 30 September 1997; and
- complete programming changes and have testing well under way for business critical systems by 31 December 1998.[68]

5.2 Survey results

The above standards were used as a baseline to establish the preparedness of Victoria's public agencies according to the Committee's Year 2000 survey results.

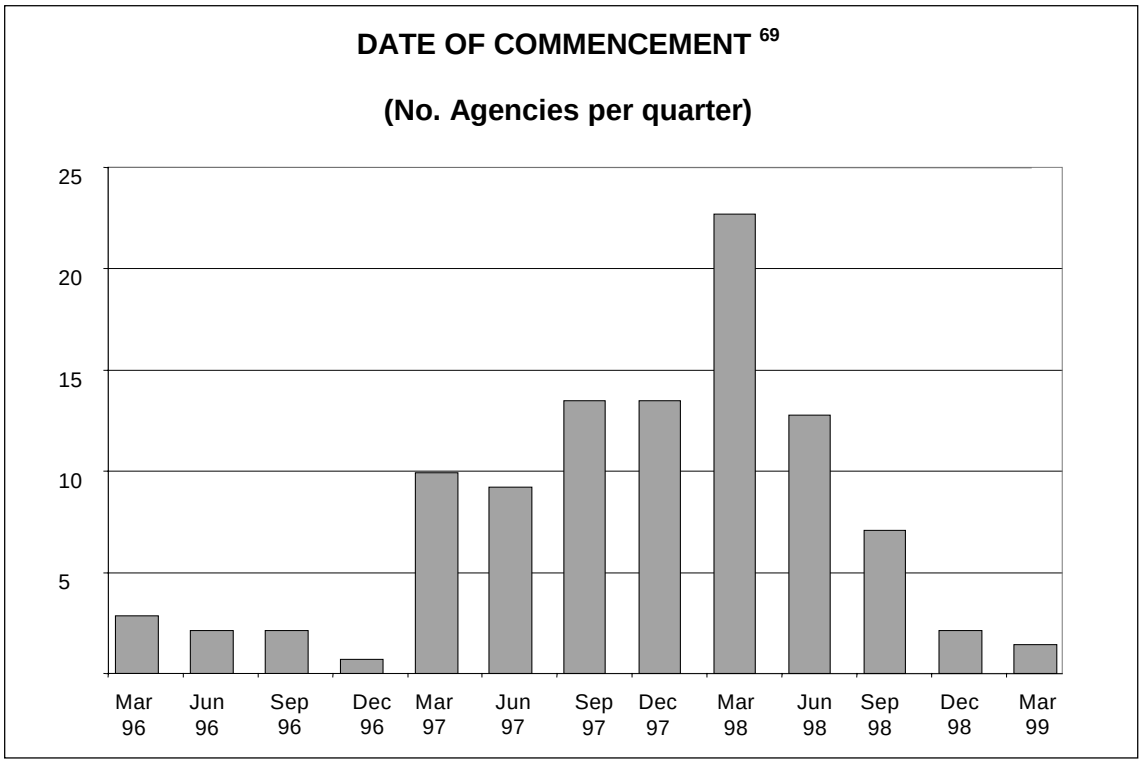
Exhibit 13 shows that 41 per cent of the 244 agencies affected by the Year 2000 problem commenced planning before 30 September 1997. However, in terms of international best practice only 9 (4 per cent) of agencies had commenced planning for the Year 2000 problem in 1996. These agencies are as follows:

- Victorian Interpreting and Translating Services;
- Royal Botanic Gardens Melbourne;
- Victorian Channels Authority;
- Council of Adult Education;
- Frankston City Council;
- Victorian Auditor-General's Office;
- Environment Protection Authority;
- Hospitals Superannuation Board; and
- Cardinia Shire Council.

The Committee concludes that most government agencies did not achieve best practice in terms of commencing Year 2000 compliance activities within an appropriate time frame.

[68] Source: Yourdon & Yourdon, op.cit. 1998, p.141.

Exhibit 13



Of more concern to the Committee are the remaining agencies, which commenced planning Year 2000 activities in 1998 and now have to make significant progress during the next couple of months. These agencies include the following bodies:

- Hospitals (36 per cent of responding hospitals);
- VicRoads;
- Metropolitan Fire Brigade;
- Public Transport Corporation;
- Regional water authorities (35 per cent of responding water authorities);
- Municipal Councils (33 per cent of responding councils);
- Victorian Financial Institutions Commission;
- State Library; and
- TAFEs (40 per cent of responding TAFEs)

a) Compliance plans

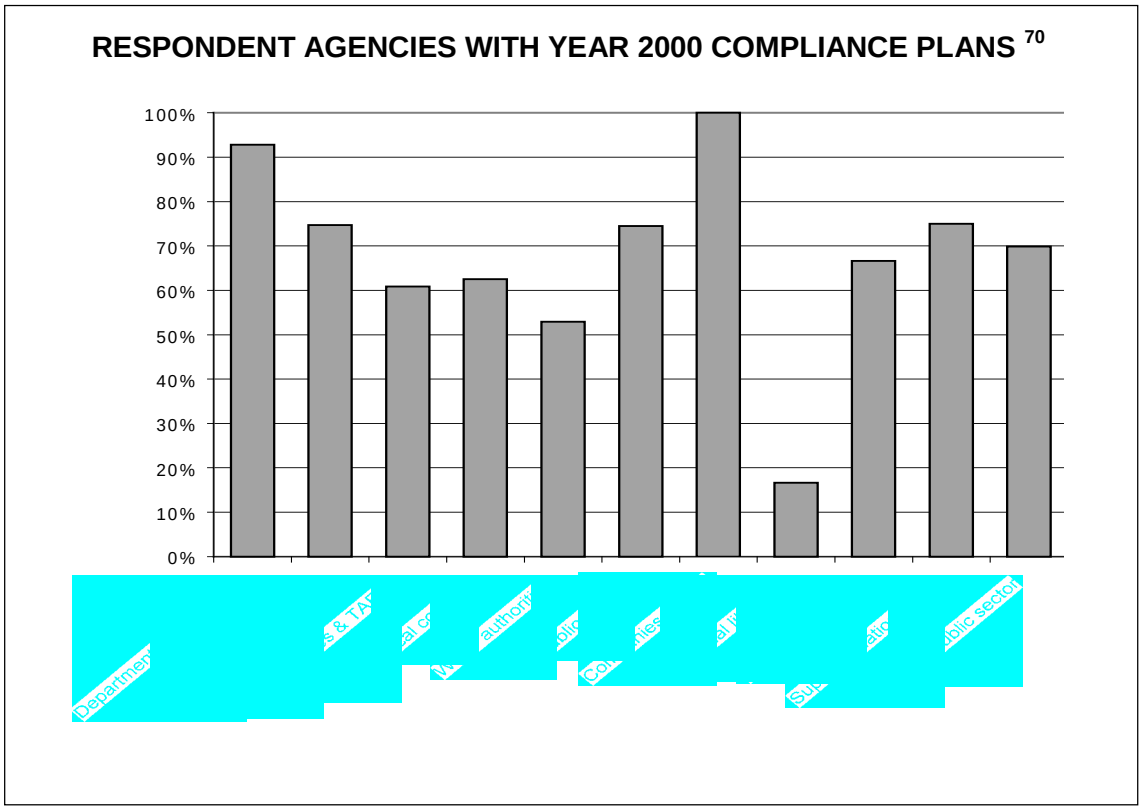
While the Committee appreciates that a comprehensive inventory needs to be prepared before priorities can be set and action plans drawn up, the

[69] Survey data for the period 3 March 1998 to 31 July 1998.

Committee is concerned about the number of agencies, particularly councils and hospitals, who indicated they will not commence planning until after September 1998.

Exhibit 14 indicates the number of respondent agencies that now have Year 2000 compliance plans.

Exhibit 14



Waste management agencies have not prepared compliance plans because they have indicated to the Committee that they have stand alone PCs which will be replaced with compliant systems prior to 31 December 1999.

The Committee is concerned that not all agencies have adopted a structured and systematic approach to the assessment of their Year 2000 problem. Agencies may have overlooked the impact of embedded chip technology on their operations eg. PABX, automatic plant equipment, security devices, fire warning and emergency shutdown systems and building control systems.

It is also the Committee's perception that smaller agencies are generally less prepared than larger agencies. A review of the survey returns indicates

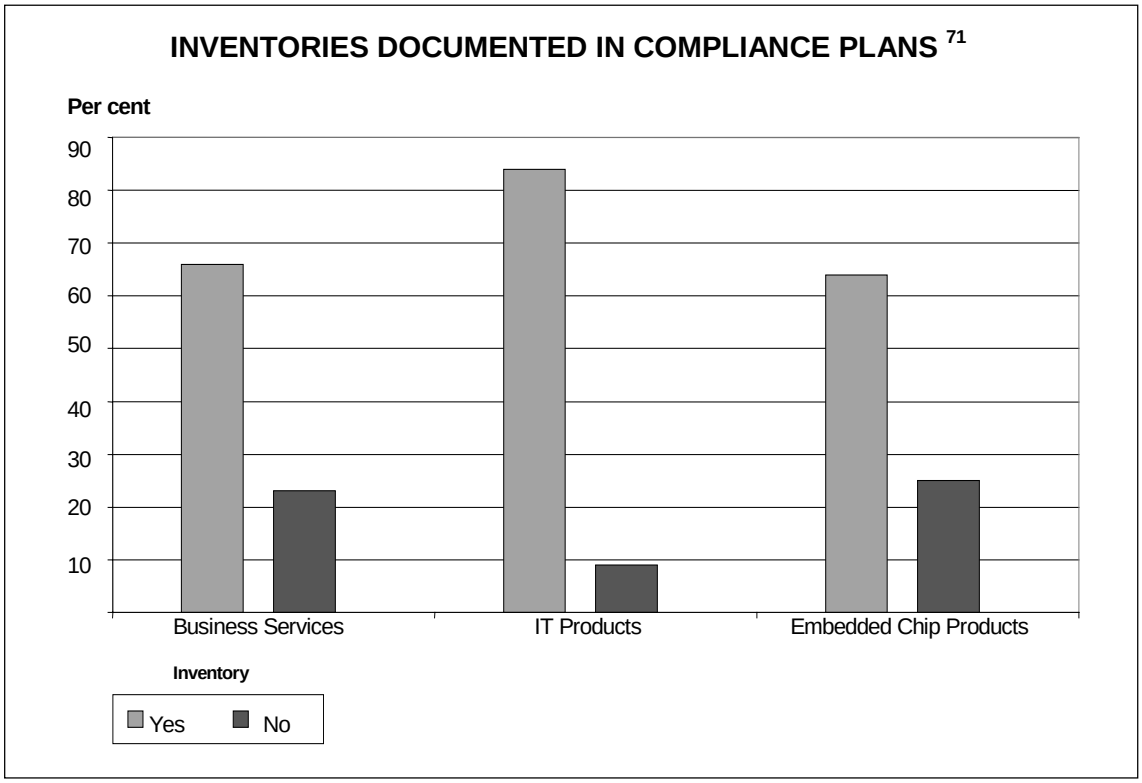
[70] Survey data for the period 3 March 1998 to 31 July 1998.

that agencies in rural areas have a lot of work to do before they will be prepared for the Year 2000 problem.

b) IT and embedded chip inventories

Exhibit 15 shows the types of inventories that have been documented in agency compliance plans. The major issues raised by these survey results concern the legal liabilities of agencies that either fail to fully document particular IT systems or overlook items which should have been checked for Year 2000 compliance. Due diligence and duty of care is further covered in Chapter 8 *Legal Implications of the Year 2000 Problem*.

Exhibit 15



It was not apparent from the responses whether agencies had identified all at-risk systems. For example, embedded systems and business services were less likely to have been included in an agency's inventory, raising concerns regarding the impact of these on business continuity.

Few returns indicated whether the assessment had been validated by internal or external auditors, or by operational staff. This is of concern because not all agencies may appreciate the potential scope or breadth of

[71] Survey data for the period 3 March 1998 to 31 July 1998.

the Year 2000 issue and some key areas of business may be exposed to the risk of interruption in 2000.

The Committee is concerned that a number of agencies had still not completed an IT inventory or prepared a compliance plan. These initiating processes must be addressed as a matter of urgency, given the limited time and resources available to these agencies to correct the problem.

c) Risk exposures

Exhibit 16 shows that 86 per cent of respondent agencies had identified their level of IT exposure and that this had been addressed in their Year 2000 plans.

Exhibit 16

RISK EXPOSURES ADDRESSED IN YEAR 2000 PLANS [72]

Public agency	*No. agencies affected*	*IT Exposure*			*Embedded Exposure*				*Business Services Exposure*			
		Yes	*%*	*No*	*Yes*	*%*	*No*	*%*	*Yes*	*%*	*No*	*%*
Departments & budget sector	14	13	93	0	11	79	2	14	11	79	2	14
Public hospitals & ambulance	72	62	86	0	52	72	8	11	50	69	9	13
Universities & TAFEs	23	20	87	0	19	83	0	0	19	83	1	4
Municipal councils	48	42	88	0	27	56	11	23	29	60	11	23
Regional water authorities	16	12	75	0	10	63	1	6	10	63	2	13
Public bodies	47	42	89	0	30	64	6	13	33	70	5	11
Companies, trusts	10	8	80	0	7	70	0	0	8	80	0	0
Regional library corporations	6	3	50	0	3	50	0	0	2	33	1	17
Public cemeteries	3	2	67	0	1	33	0	0	2	67	0	0
Superannuation funds	4	4	100	0	4	100	0	0	3	75	1	25
Waste management groups	1	1	100	0	1	100	0	0	1	100	0	0
Total public sector	**244**	**209**	**86%**	**0**	**165**	**68%**	**28**	**11%**	**168**	**69%**	**32**	**13%**

Exhibit 16 also indicates that 23 per cent of local councils and 11 to 13 per cent of hospitals had not included risk exposures in relation to embedded chip equipment or business services.

For hospitals such risk exposures could include interruptions to the business supply chains that provide pharmaceuticals, medical supplies, linen services, meals and food, laboratory and medical equipment and radiology and pathology services.

[72] Survey data for the period 3 March 1998 to 31 July 1998.

d) Approach to Year 2000

Exhibit 17 outlines the approach to be adopted by agencies in addressing the Year 2000 problem.

Exhibit 17

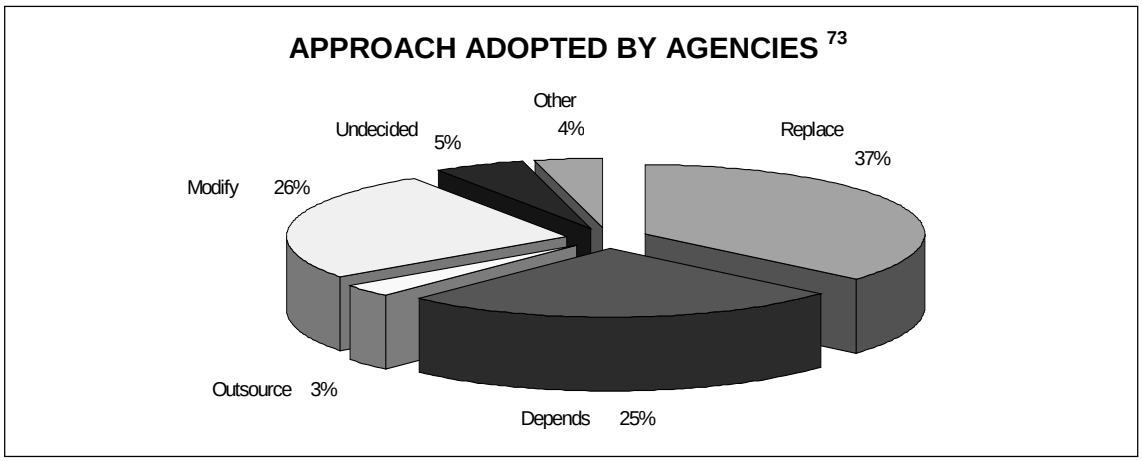
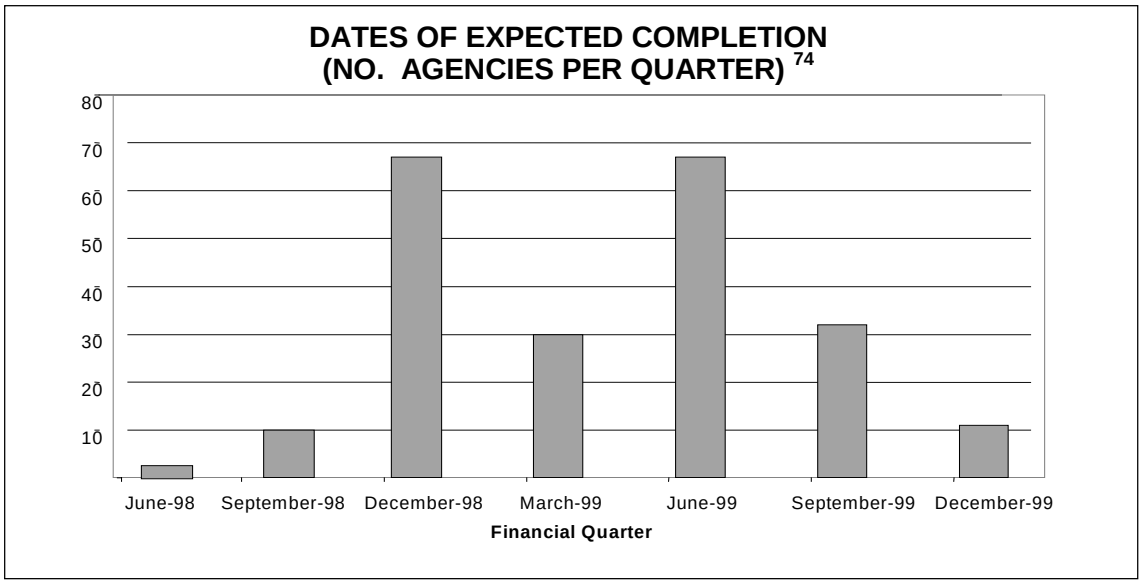


Exhibit 17 shows that a third of agencies affected by the Year 2000 problem were either undecided or had not completed their assessment, about a quarter will modify their IT systems and over a third will replace their systems with compliant versions. This supports other data supplied by respondent agencies which indicates that Year 2000 compliance had not progressed past the planning and assessment stage during the June quarter of 1998.

e) Date of expected completion

Exhibit 18 shows the expected date of completion of Year 2000 compliance plans.

Exhibit 18



[73] Survey data for the period 3 March 1998 to 31 July 1998.
[74] Survey data for the period 3 March 1998 to 31 July 1998.

Exhibit 18 shows that, of the 244 respondent agencies, fewer than half were expected to be compliant by the end of 1998. The remaining agencies were expected to be compliant by 30 June 1999 or 30 September 1999 or had not determined when they would achieve compliance. In terms of business critical systems, the Minister responsible for the Government's response to the Year 2000 problem advised the Committee that the intention was that all agencies would be compliant by 31 December 1998.[75]

In terms of best practice, the vast majority of Victorian public sector agencies have not commenced Year 2000 compliance activities in the best possible time frame. Consequently, as indicated in the following Chapter "*Implementation, Monitoring and Management Strategies*" most agencies may not have time to complete implementation, which includes the critical and time consuming step of testing changed systems before the end of 1999.

The Committee recommends that:

Recommendation 5.1:	***The Government establish spot checks by appropriately qualified auditors on the progress of all essential infrastructure service providers against Year 2000 compliance targets.***

Recommendation 5.2:	***If it becomes apparent that some business critical systems will not be fully compliant by key dates, Government ensure that adequate contingency plans are developed and tested[76] to guarantee business continuity and the continuation of government service provision.***

Recommendation 5.3:	***The Government focus on critical areas where planning and progress to date shows that improvement is needed.***

Recommendation 5.4:	***The State's disaster response plan (DISPLAN) be reviewed to take into account the possibility of simultaneous disasters arising from the Year 2000 problem.***

[75] PAEC Budget and Estimates hearing, The Hon. Roger Hallam, Minister for Finance, 27 July 1998, p.37.

[76] The Committee is aware of community Year 2000 simulation exercises conducted in the US. For example, in Lubbock, Texas, in *The Australian*, 6 October 1998, p.5.

Chapter 6:
Implementation, Management and Monitoring Strategies

"The closer you look at it the larger the task is, the more questions we ask, the more people realise that they have got a more serious issue on their hands." [77]

6.1 Introduction

The progress of Year 2000 project implementation across Victorian public sector agencies has been assessed in terms of the stage at which the majority of Year 2000 compliance activities fall. The four phases of Year 2000 project implementation are as follows:

a) Planning Phase

The planning phase involves the compilation of complete inventories of hardware, software, agency business systems and embedded systems used in business critical business functions. An agency business system inventory is a list of business critical suppliers, for example, Qantas identified 200 business critical suppliers including aircraft manufacturers, network service providers, fuel suppliers, key business partners and banks.[78.]

b) Assessment Phase

Each item in the inventory is assessed for its Year 2000 compliance. Risks are evaluated and priorities assigned to reduce the risk to business critical processes. Resource requirements are identified in terms of the cost, personnel and timings needed to remedy Year 2000 problems. Plans are developed to address the identified risks and contingency plans are prepared to ensure business continuity in the event of persistent Year 2000 problems after 31 December 1999.

c) Conversion Phase

Conversion refers to the modification of computer code or the replacement of software or hardware to remedy the Year 2000 problem. Decisions on conversion strategy should be made on business grounds rather than a technical basis. The replacement of some applications, for example, may be accelerated to avoid dependence on third party software or unduly expensive

[77] Mr Mike Harrington, Director Special Projects, Department of Premier and Cabinet, PAEC Private hearing, 11 May 1998, p.29.
[78] The *Australian Financial Review*, 23 June 1998, p.40.

conversion costs. Masking techniques are favoured for low volume applications likely to be replaced within a few years.

d) Implementation Phase

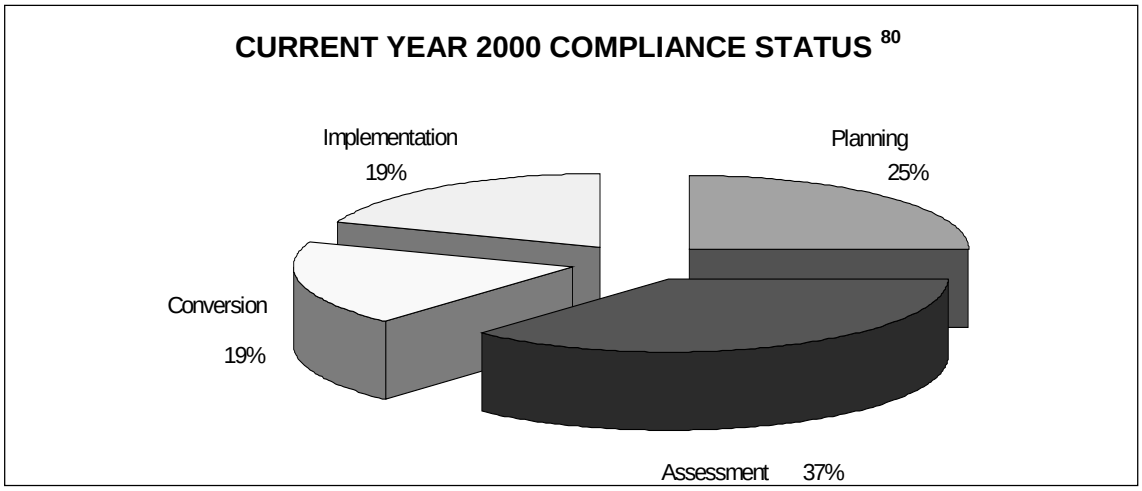
This is the most important phase in terms of ensuring business continuity as all changed systems and applications are tested under simulated real life conditions. 'Real life' conditions refer to the advancement of the date in computer systems or embedded chip[79] systems to test for compliance. Any errors in programming are detected and corrected and then re-tested until the remediated IT system and its software applications are fully Year 2000 compliant. Contingency plans and disaster recovery plans are reviewed and updated during this phase.

According to international best practice the costs of inventory, analysis and conversion should be about 50 per cent of an agency's total Year 2000 compliance project costs and 50 per cent should be devoted to the final testing phase. The final testing phase is the most time-consuming and critical phase of Year 2000 compliance.

6.2 Survey Results

Exhibit 19 indicates the Year 2000 compliance project status of respondent agencies during the survey. The data on project status was aggregated as most agencies indicated that more than one phase was in progress, therefore, the percentages shown reflect the total proportion of each compliance activity across the whole of government. The figures do not represent the number of agencies in each phase.

Exhibit 19



[79] The manufacturer of the embedded chip or device should be consulted before advancing dates on embedded chip systems as such tests can ruin equipment.

[80] Survey data for the period 3 March 1998 to 31 July 1998.

The Committee is concerned that 37 per cent of agency project activity was still in the assessment phase and 25 per cent was in the planning phase. Together 62 per cent of public sector Year 2000 project activity was devoted to the compilation of IT inventories and the assessment of the extent of the Year 2000 problem. In accordance with international best practice this activity should have been completed in 1997 to permit enough time to fix and test IT systems throughout 1998 and 1999.

The Committee appreciates that there have been significant developments since responses to the questionnaire were prepared in the June quarter of 1997-98. These include:

- the establishment of the Year 2000 Risk Management Unit, Department of Treasury and Finance, to monitor the progress of agencies' compliance activities;
- regular reporting to Cabinet on progress made by agencies; and
- the direction that agencies must include a statement in their annual report about progress achieved against their Year 2000 compliance plan.

The Committee believes that these initiatives have given much needed impetus to the process and ensure commitment and leadership by senior management in addressing the issues associated with achieving compliance for key critical systems.

6.3 Managing business critical services

The Committee met with representatives from the gas, electricity and water utilities and officers involved with the Year 2000 problem from the following agencies:

- Office of the Regulator-General (overview of regulated industries);
- United Energy and SMS Consulting Pty Ltd (electricity industry);
- VENCorp (gas industry);
- Melbourne Water Corporation (water supply and sewerage disposal);
- Telstra Corporation (telecommunications);
- Department of Human Services (hospitals and health services);
- Department of Justice (corrections, police and emergency services);
- Public Transport Corporation (buses, trains and trams); and
- Department of Infrastructure (local government and municipal councils).

The Committee received evidence on the progress of Year 2000 compliance projects in the business critical systems of these key service providers. All were confident that they would meet their deadlines for Year 2000 compliance.

The Committee was concerned however, that many utilities and agencies had yet to complete their inventories or fully examine their exposure to external parties. The electricity industry, for example, had invested up to $15 million to date on the planning and assessment phases and had yet to commence the conversion and implementation phases.[81] Melbourne Water had completed inventories for IT and embedded chip systems and was 40 per cent of the way through assessing the extent of the problem for the inventoried embedded chip systems.

The Committee appreciates that because of possible legal ramifications and commercial confidentiality considerations, many of the utilities have been reluctant to reveal information about their level of compliance.

6.4 Industry coordination

The Committee understands that recent action has been taken to establish industry groups for electricity, gas and water, hospitals and local councils:

- the Victorian Electrical Supply Industry Year 2000 Group (VESI) was established in July 1998 to address the high interdependence of electricity suppliers in the Victorian electricity industry. Relatively small Year 2000 failure events, when combined under certain circumstances, could possibly cause failure of the power supply system;
- VESI recently appointed a coordinator to facilitate communication between participants in Victorian electricity to support current Year 2000 compliance efforts. The coordinator will advise on the progress of Year 2000 compliance to stakeholders such as the Regulator-General, the Electricity Supply Association of Australia (ESAA), customers and the National Electricity Market Management Company (NEMMCO);[82]

[81] PAEC Private hearing, 21 August 1998, p.8

[82] The National Electricity Market Management Company (NEMMCO) was established by the State Governments to manage the wholesale electricity market on behalf of the NSW, ACT, Victoria, South Australia and Queensland. NEMMCO commences its takeover on 15 November 1998 *http://electricity.net.au/nemmcorol.htm.*

- seven gas network operators: AGL, Stratus, Multinet, Westar, Alinta, Allgas and Envestra met in Canberra to hear from the Year 2000 Taskforce;[83]
- a Local Government Year 2000 Working Group has been established by the Department of Infrastructure to advise councils on the Year 2000 problem and to provide a forum for sharing solutions;
- the Department of Human Services has established statewide forums for Year 2000 Coordinators and Year 2000 Medical Engineers; and
- the Centre for Biomedical Engineering, Monash University is coordinating a biomedical equipment compliance database in hospitals, funded by the Department of Human Services.

While the Committee welcomes these developments, it remains concerned that so much must be achieved within a fixed timeframe. For example, there are 90,000 medical equipment devices in hospitals, of which 85 per cent are business critical. Even though only a small percentage of these devices will be affected, each item must be checked, tested and possibly repaired or replaced within the remaining time.[84]

No matter how confident agencies are of the success of their Year 2000 program, there is absolutely no certainty that problems will not occur. If key systems such as water, electricity or telecommunications fail the social and economic ramifications would be serious. Any major failure of the electricity generation, transmission or distribution systems has the potential to cause more disruption to Victoria than any other single infrastructure element.

6.5 Monitoring Year 2000 compliance

The Government has recently introduced a unit to monitor the central oversighting and reporting of agencies' progress towards Year 2000 compliance. This will involve agencies reporting to Cabinet through the Year 2000 Risk Management Unit every month. This reporting framework includes an audit of agency compliance activity to provide the appropriate assurances to Cabinet.

The Committee was also informed that the Office of the Regulator-General is currently establishing an audit process for the electricity industry in order to gain assurances regarding the industry's state of preparedness. The Regulator has licensing and regulatory powers covering most of the

[83] *The Australian Financial Review*, 12 October 1998, Special Report, p.37.
[84] 0.5% to 2.0% *In* 'Attachment 3: High Risk Areas', Department of Human Services, PAEC private hearing, 10 September 1998.

electricity industry, including the generation, transmission, distribution and retail sectors. However, the Regulator does not have the regulatory oversight role in relation to NEMMCO, the national market operator with responsibility for ensuring security of supply in the multi-state electricity market to be in operation before 1 January 2000. Coordination and oversight of the interstate aspects of Year 2000 preparedness is undertaken by a Commonwealth Standing Committee of officials under the auspices of ANZMEC.

Currently the Regulator-General has licensing and regulatory powers only in relation to the distribution and retail sectors of the gas industry and the metropolitan distribution and retail water businesses. In view of the Office's partial regulatory coverage of the gas and water industries and the ongoing reform processes in those industries, the responsible Departments should have the oversight of their Year 2000 preparedness. Overall the Regulator-General as at August 1998 did not have an overview of Year 2000 issues for the gas, water or electricity industries in Victoria.[85]

The Committee believes that it is essential that the risks to the operations of government and the consequences and impacts on the community are prioritised and ranked from a whole of government perspective so that adequate funding and resources can be allocated to the most critical systems.

The Committee believes that the Year 2000 Risk Management Unit should recommend the allocation of resources based upon a whole of government risk management strategy. This will be particularly important, if it becomes apparent towards the middle of 1999 that certain business critical areas will not achieve compliance. Where the consequences of potential non-compliance are assessed by the Year 2000 Risk Management Unit as likely to cause widespread problems for business continuity or the community, appropriate resources should be made available without delay.

6.6 Real life compliance testing

Real life compliance testing refers to Year 2000 compliance tests where the date is advanced to suspect or random dates in order to detect potential failures or problems in new or changed IT environments. Exhibit 20 shows the results of the Year 2000 survey and indicates the level of real life compliance testing for the various risks associated with the Year 2000 problem.

[85] PAEC private hearing, 21 August 1998, p.22.

Exhibit 20

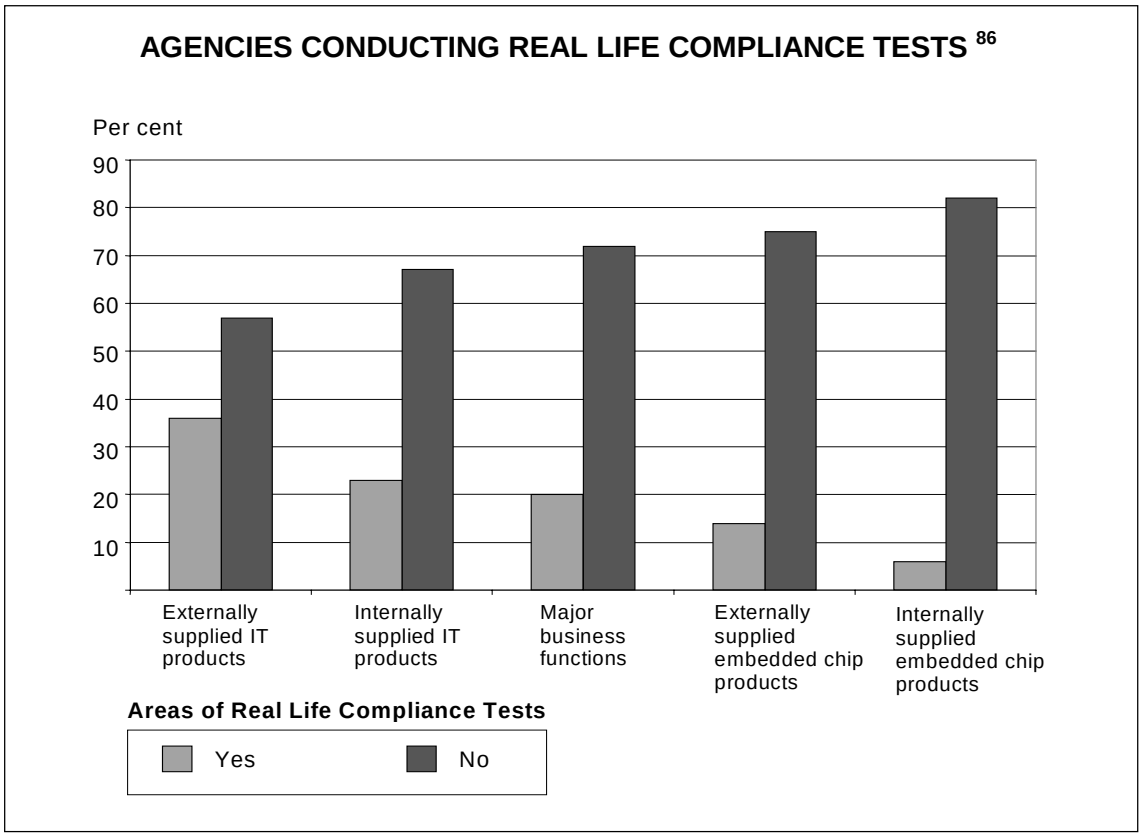


Exhibit 20 shows that only a third of agencies had conducted real life compliance tests on externally provided IT products, with lower proportions recorded for other Year 2000 related problem areas. The low incidence of testing is indicative of the planning and assessment phases in which most agencies were involved at the time of the Committee's survey.

Exhibit 20 also shows, however, that there is a propensity for agencies to ignore the need for testing major business functions and embedded chip products. Both of these elements have the capacity to disrupt normal business operations across all agencies during the year 2000.

The need for testing is of concern given the tight time frames that most agencies have now imposed on themselves. For example, in terms of reprogramming computer code:

> *"the chances for error are much greater when:*
>
> - *working under extreme pressure;*
> - *modifying a computer program written by someone else;*

[86] Survey data for the period 3 March 1998 to 31 July 1998.

- *working in a program language with which one is not particularly familiar or experienced; and*
- *working on a program for which there is no current documentation.*

These four conditions are exactly what most Year 2000 projects face." [87]

The Committee has previously referred to testing as the most important step in a Year 2000 compliance program. This is because if testing is either not conducted or not conducted thoroughly, the investment of time and vast resources put into solving the Year 2000 problem could well be wasted. The Year 2000 problem may persist until all date-related problems are eliminated, as even small date-related errors can cause the loss of business continuity.

6.7 Project management

Exhibit 21 shows the proportion of agencies that have established critical milestones against which the progress of their Year 2000 compliance projects can be evaluated.

Exhibit 21

AGENCIES WITH CRITICAL YEAR 2000 PROJECT MILESTONES [88]

Public agency	*No. agencies affected*	*Critical milestones*			
		Yes	*%*	*No*	*%*
Departments & budget sector agencies	14	13	93	1	7
Public hospitals & ambulance services	72	43	60	25	35
Universities & other educational institutions	23	14	61	7	30
Municipal councils	48	30	63	14	29
Regional water authorities	16	11	69	3	19
Public bodies	47	27	57	13	28
Companies, trusts & joint ventures	10	6	60		0
Regional library corporations	6	2	33	2	33
Public cemeteries	3	2	67	1	33
Superannuation funds	4	3	75		0
Regional waste management groups	1	1	100		0
Total public sector	**244**	**152**	**62**	**66**	**27**

[87] Yourdon, E.& J. Yourdon, '**Time Bomb 2000** What the Year 2000 Computer Crisis Means to You'. Prentice Hall, N.J. , 1998, p.116.
[88] Survey data for the period 3 March 1998 to 31 July 1998.

The Committee was pleased that almost all of the inner budget agencies showed good management practice by establishing critical project milestones for their Year 2000 program. However, one third of the State's public agencies had not established project milestones and were consequently at risk of falling behind schedule.

Exhibit 22 shows the number of agencies at the time of the survey that were on schedule to complete their Year 2000 compliance projects according to plan.

The Committee believes that the results are optimistic given that a third of the agencies had not established clear markers against which progress could be measured. Indicative of this, approximately ten per cent of agencies did not answer this question in the survey.

Exhibit 22

AGENCIES WITH YEAR 2000 COMPLIANCE PROGRAMS ON SCHEDULE [89]

Public agency	*No. agencies affected*	*Agencies on schedule*	*%*	*Agencies not on schedule*	*%*	*Not answered*	*%*
Departments & budget sector	14	13	93	1	7		
Public hospitals & ambulance	72	49	68	17	24	6	8
Universities & TAFEs	23	18	78	2	9	3	13
Municipal councils	48	40	83	3	6	5	10
Regional water authorities	16	11	69	3	19	2	13
Public bodies	47	39	83	5	11	3	6
Companies, trusts & ventures	10	7	70		0	3	30
Regional library corporations	6	4	67		0	2	17
Public cemeteries	3	3	100		0		0
Superannuation funds	4	3	75		0	1	25
Waste management groups	1	1	100		0		0
Total public sector	**244**	**188**	**77**	**31**	**13%**	**25**	**10**

The Committee was encouraged by the confidence expressed by most agencies (77 per cent) that Year 2000 compliance programs were on schedule. These results provide a balance to benchmark comparisons, which show that most agencies started their Year 2000 compliance activities at a late stage.

The Committee is adamant that agencies should thoroughly test new IT environments, including embedded systems, as early as possible.

[89] Survey data for the period 3 March 1998 to 31 July 1998.

The Committee found that there is an important role for auditors to monitor and report on the processes and expenditures undertaken by agencies on Year 2000 compliance programs. Although qualified IT auditors are also needed to verify the Year 2000 remedies implemented by agencies, the Committee notes a general reluctance by auditing firms to undertake Year 2000 compliance testing.

6.8 Leadership

Exhibit 23 shows the number of agencies that have established a Year 2000 task force.

Exhibit 23

PUBLIC SECTOR AGENCIES WITH YEAR 2000 TASK FORCES [90]

Public agency	*No. agencies affected*	*No. with Year 2000 task forces*	*%*
Departments & budget sector agencies	14	11	79
Public hospitals & ambulance services	72	51	71
Universities & other educational institutions	23	21	91
Municipal councils	48	27	56
Regional water authorities	16	11	69
Public bodies	47	28	60
Companies, trusts & joint ventures	10	10	100
Regional library corporations	6	2	33
Public cemeteries	3	2	67
Superannuation funds	4	4	100
Regional waste management groups	1	0	0
Total public sector	**244**	**167**	**68**

Exhibit 23 indicates that the majority of public agencies have established project task forces to address the Year 2000 problem across their respective organisations. The survey returns also indicate that most of the Year 2000 project task forces report to senior levels within their organisations, therefore, enhancing the accountability process for Year 2000 project outcomes.

These results inform the Committee that project management is generally well planned across the public sector for those agencies that have commenced Year 2000 projects. The Committee is concerned, however, that a third of municipal councils, public hospitals, regional water authorities and public bodies had not established project task forces to deal with the Year 2000 problem. These survey results correlate with the results

[90] Survey data for the period 3 March 1998 to 31 July 1998.

for agencies without compliance plans; that is, almost a third of these particular agency types had not commenced any Year 2000 project initiatives.

The internal and external resources engaged by agencies to form Year 2000 project task forces are shown in Exhibit 24:

Exhibit 24

RESOURCES ENGAGED TO FORM YEAR 2000 TASK FORCES [91]

Public agency	*No. agencies with Taskforces*	*Both Internal and External resources*			
		Yes	*%*	*No*	*%*
Departments & budget sector agencies	11	9	82	1	9
Public hospitals & ambulance services	51	35	70	17	33
Universities & other educational institutions	21	5	24	11	52
Municipal councils	27	16	59	8	30
Regional water authorities	11	6	55	5	45
Public bodies	28	16	57	13	46
Companies, trusts & joint ventures	10	4	40	1	10
Regional library corporations	2		0	2	100
Public cemeteries	2	2	100		0
Superannuation funds	4	1	25	3	75
Regional waste management groups	0		0		0
Total public sector	**167**	**94**	**56**	**62**	**37**

Exhibit 24 indicates that just over half of the Year 2000 task forces in the public sector use both internal and external resources. This suggests to the Committee that there is a high reliance across the public sector on the availability of external IT consultants to address Year 2000 problems in agencies.

Further analysis of the survey results for task force resources is shown in Exhibit 25.

[91] Survey data for the period 3 March 1998 to 31 July 1998.

Exhibit 25

RESOURCES USED IN AGENCY TASK FORCES [92]

Public agency	*No. agencies with Taskforces*	*No. Internal resources*	*No.External resources*	*Ave. Resources per Task force*	*Ratio Internal/ External*
Departments & budget sector	11	117	15	12	7.8
Public hospitals & ambulance	51	183[(a)]	28[(b)]	4.1	6.5
Universities & TAFEs	21	41	3	2.1	13.6
Municipal councils	27	89	26	4.25	3.4
Regional water authorities	11	34	8	3.8	4.25
Public bodies	28	64	38	3.6	1.7
Companies, trusts & ventures	10	77	4	8.1	19.25
Regional library corporations	2	0[(c)]	0	0	0
Public cemeteries	2	1	7	4	0.14
Superannuation funds	4	3	1	1	3
Waste management groups	0	0	0	0	0
Total public sector	**167**	**609**	**130**	**4.4**	**4.7**

Notes:
(a) The Regional Alliances Strategy developed by the Department of Human Services has caused a duplication of the figures for both internal and external resources, which are shared between groups of individual rural hospitals.
(b) External resources for rural hospitals include IT staff from the Department of Human Services.
(c) The resources allocated to these 2 task forces were not given.

Exhibit 25 shows that:

- on average there are nearly five times as many internal to external resources used to form Year 2000 task forces across the public sector. Major deviations above the average occur for State-owned companies, trusts and joint ventures and universities and TAFEs; these agencies have placed less reliance on the use of external resources;
- major deviations below the internal/external ratio occur for councils, public bodies and public cemeteries. These agencies have placed a greater reliance on external consultants relative to available internal IT resources;
- the average task force is comprised of a team of four people with far larger teams in Departments and companies, trusts and joint ventures; and
- the Regional Alliance Strategy of the Department of Human Resources has proved to be an efficient method for resourcing Year 2000 task forces across the rural hospital system.

[92] Survey data for the period 3 March 1998 to 31 July 1998.

The Committee believes that the present reliance on external resources will grow. The pressure points as shown in the above analysis will mainly affect councils and public bodies. To avoid the foreseeable lack of external resources available to these bodies the Committee recommends the sharing of resources and the formation of a central pool of IT resources for common use across these areas. This strategy has been adopted by the Department of Human Services for rural hospitals through the formation of regional alliances and the pooling of the Department's IT resources.

The Committee notes that the Year 2000 Risk Management Unit is establishing a government panel contract of external IT consultants to address the Year 2000 problem and that the contract will be available to local councils. In light of the Committee's survey results, this is a much-needed initiative that should improve the public sector's progress towards Year 2000 compliance.

6.9 Retention of IT resources

The Year 2000 problem is mainly found in software applications and consequently its timely resolution is heavily dependent upon the availability of IT resources with expertise in computer programming. Programmers of legacy systems mainly require skills in Common Business Orientated Language (COBOL).[93]

The Committee notes that computer analyst programmers, however, are in short supply throughout Australia,[94] and in an environment of increasing demand for Year 2000 problem solving skills, that the cost of computer consultants will increase in 1999.

The Committee's survey indicates that up to 64 per cent of government departments, inner budget agencies and public sector bodies have decided to modify their current computer systems. To avoid the expected escalation in programming costs, particularly after 31 December 1998, this strategy is reliant upon the retention of IT expertise within the public sector.

The current trends in IT staffing issues in the public sector are unknown, however, given the government's recent trend towards outsourcing IT services, the Committee is concerned any downward trends could impact on IT staff availability. A shortage of skilled IT professionals in the public sector prior to the conclusion of the government's Year 2000 compliance activities would exacerbate the potential risks of the Year 2000 problem.

[93] Yourdon, E and Yourdon, J 'Time Bomb 2000: What the Year 2000 Crisis means to you!' Prentice Hall PTR Upper Saddle River, New Jersey 1997, p.189.
[94] *The Australian*, 22 September 1998, p.53.

The Committee is also aware of recent initiatives by the Queensland Government to provide incentives to government IT staff of a 20 per cent cash bonus if they see an IT project through to completion. This initiative was taken following a sharp increase in the number of IT staff leaving the public sector to take up better paid positions in the private sector for Year 2000 compliance work.[95]

The Committee recommends that:

Recommendation 6.1:	***The Government expand the 'spot checking' audit function of the Year 2000 Risk Management Unit to focus its verification reports on the essential services – gas, water, electricity, emergency communications and the major hospital networks.***

Recommendation 6.2:	***As a matter of priority, resources be made available to enable business critical systems to be made compliant. Contingency plans need to be coordinated across the hospital system to cater for all emergency eventualities***.

Recommendation 6.3:	***To encourage the sharing of information, the appropriate agency organise forums for agencies and industries that are likely to share common Year 2000 problems eg. the emergency services, SMEs, water, gas and electricity retailers and distributors, electricity generators and transmission companies.***

Recommendation 6.4:	***That similar agencies such as those in local councils or water management authorities be encouraged to share IT resources for remediating common Year 2000 problems.***

Recommendation 6.5:	***Agencies verify whether their contingency plans are sufficient to ensure business continuity and the maintenance of adequate levels of service in the event of multiple failures.***

[95] *The Australian*, 13 October 1998, p.35.

The Committee recommends that *(continued)*:

Recommendation 6.6:	***The annual report data on year 2000 compliance activities for 1997-98 be centrally collated by the Year 2000 Risk Management Unit as a means of measuring the progress of public agencies since the Public Accounts and Estimates Committee survey.***

Recommendation 6.7:	***All agencies thoroughly test new IT systems and IT equipment under real life conditions to ensure the proper completion of year 2000 compliance activities.***

Recommendation 6.8:	***The government develop IT staff retention strategies to ensure the retention of IT personnel with the appropriate skills for year 2000 related work.***

Chapter 7: Service Agreements and Contracts

"Even if they signed off that they were Year 2000 compliant you could never be positive that that was the case." [96]

7.1 Introduction

Service agreements and contracts relating to the purchase of new IT equipment or the provision of IT services, need to include specific warranties or indemnities to protect the Government.

The Committee was advised that due to the foreseeable nature of Year 2000-related problems the insurance industry would not provide coverage for clients in either the private or public sectors.[97]

The government's Year 2000 Policy issued in July 1996 included several model clauses that were to be written into all IT purchase orders and IT contracts entered into by inner budget agencies. The Committee was advised, however, that these clauses were not always included in purchase contracts and that most departments now rely on the standard general conditions of supply contracts which provide remedies for breaches of supply conditions.[98]

The Victorian Government Purchasing Board (VGPB) develops supply management policies and guidelines for departments to manage purchasing and contracting. The Board's standard contract for IT services, the Government Information Technology Conditions, version 2 (GITC2) does not include specific provisions to protect agencies in the event of Year 2000-related computer problems.

The Committee was also surprised to learn that some very large service agreements under the government's recent outsourcing and privatisation programs do not have any specific protection or indemnities against Year 2000 related problems.[99] The Committee understands that some of these contracts have been renegotiated and amended to require the current contractors to remediate the Year 2000 problem, but at significant extra cost to the government.

[96] PAEC private hearing, 12 August 1998.
[97] For example, PAEC private hearings, 12 August 1998 (e.g. OGIT) and 14 September 1998 (e.g. Mr Graeme Inchley, Chief Executive officer, Federal Y2K Industry Program).
[98] For example, PAEC private hearings on 28 August 1998 (VicRoads, p.13) and 11 September 1998.
[99] For example, the Intergraph contract, PTC (mainframe and Onelink contracts). PAEC private hearings, 28 August 1998, 10 & 11 September 1998.

7.2 Contract requirements

The Committee understands that some attempts have been made to deal with Year 2000 liability in contracts with consultants and suppliers. The success of these clauses is dependent upon a number of factors, including:

- whether such clauses are in fact included in the contract, i.e. many model clauses have been developed solely for use in IT-related contracts, whereas Year 2000 issues may arise in respect of goods and services not regarded as IT-related;
- the drafting of the specification. This will affect issues such as compliance with description, performance standards and warranties; and
- whether contractual obligations on the supplier, such as requiring them to obtain insurance, have been monitored and enforced.

It is essential that in purchasing any new goods or services, agencies ensure that a warranty is sought regarding Year 2000 compliance, i.e. the product will continue to function properly beyond 1999 and that there will be no interruption or delay in the supply of services beyond that date.

Because of potential liability, existing contracts should be reviewed with particular consideration to the following matters:

- warranties made regarding the nature and performance of the services and products, in particular, that the services and products are clearly intended to function beyond 1999;
- the drafting of the specification;
- any exclusions or limitations on liability; and
- indemnities.

7.3 General conditions for supply of goods and services

The VGPB has issued *General Conditions for Supply of Goods and Services to Departments.* This contract is used by all inner budget agencies when purchasing goods and services. No specific reference is made in the contract to the Year 2000 issue.

The indemnity clause (clause 13) provides that:

> *"The Contractor releases and indemnifies the Department its servants and agents from and against all damages, costs, expenses, loss or damage which they may incur or sustain, actions, proceedings, claims and demands whatsoever which may be brought or made against them by any person in respect of or by reason of or arising out of:*

- *the provision of goods or services by or on behalf of the Contractor;*
- *any negligence or other wrongful act or omission of the Contractor or its employees, agents or subcontractors or of any other persons for whose acts or omissions the Contractor is vicariously liable;*
- *any negligence or wrongful act or omission of the Contractor's visitors, invitees or licensees;*
- *death, injury, loss of or damage to the Contractor, the Contractor's employees, agents, visitors, invitees, licensees or sub-contractors; and*
- *any breach of this agreement by the Contractor."*

The clause provides broad coverage in relation to any damage suffered by a Department arising from the supply of goods or services by a contractor.

The Committee notes that the viability of bringing an action against a supplier under this indemnity will depend upon the supplier's solvency and that there is a three-year limit on insurance (clause 14) under these conditions.

Clause 8 contains a general warranty that

> *"If a defect (fair wear and tear excepted) appears in the goods within the warranty period [to be defined] the Contractor shall promptly remedy such defect by either repairing or replacing defective goods without cost to the Department"*.

In addition, where provided in the specification the Contractor must

> *"obtain for the Department the benefit of any manufacturer's warranty"*.

The Committee was advised that a Year 2000 problem might be legally challenged if it is regarded as a "defect" and that this may depend largely on the drafting of the specification. If a software product, for example, is date dependent and clearly intended for operation beyond 1999, any failure to operate beyond that date may in fact be a defect. The older the product, the less likely it is that this argument will be successful. It would also be necessary to clarify the term of the applicable warranty period. Additional warranties are contained in clause 10, relating specifically to fitness for purpose, conforming to the specification, freedom from defects and that the goods are of merchantable quality and conform to any legally applicable standards.

A further problem is the issue of knowledge and waiver of any Year 2000 problem by a Department. For example, if it is considered that a Department knew of any Year 2000 problem and did not specifically address the issue, it may be considered to have accepted the known risk of Year 2000 failure.

The extent of protection may also depend upon the definition given to the terms "goods" and "services". It is therefore essential for any description of goods and services in the specification to require Year 2000 compliance.

Clause 6 provides for acceptance testing of the goods by the Department. The Department may reject goods that do not comply with the specification, however, if the goods are not accepted or rejected by the Department within 30 days they are deemed to have been accepted. Upon acceptance, ownership and risk of the goods passes to the Department.

Due to these specific issues and the fact that the agreement may incorporate other terms and conditions under clause 2, each case would need to be considered on an individual basis. Other issues may include whether the failure:

- is due to the particular goods or services; or
- relates to interoperability with other equipment or data failures.

Care in drafting the specification is therefore crucial to providing the correct levels of protection for the Government against Year 2000 problems. In general the Committee believes that the contract offers a basic, though uncertain, level of comfort.

7.4 Agreement for professional services

The VGPB has issued the *Agreement for Standing Offer for Professional Services* that is used by all inner budget agencies when contracting professional services. There are no specific references in the agreement to the Year 2000 issue.

The Committee notes that the agreement contains an "Entire Agreement" clause (clause 2), which means that the specific agreement document contains the entire terms of the contract in relation to the subject matter of the agreement. For example, all previous correspondence, representations and warranties are specifically excluded and any subsequent Year 2000 compliance statements cannot be relied upon as part of the agreement, unless specifically incorporated by both parties.

Pursuant to clause 11 the Contractor warrants that the project services shall be carried out with all due care and skill and in accordance with the highest

applicable professional standards, principles and practices. The Contractor is also obliged to comply with any relevant quality assurance standards, specified in Schedule 2.

As with the previous agreement, there is some scope for legal argument regarding compliance with these standards in the event of Year 2000 failure. This will need to be considered on a case by case basis in terms of the services provided, when it was provided, the specifications, duration and interoperability with other services.

The drafting of service specifications will be of key importance in assessing the Government's liability. For example, Clause 4.4 contemplates the inclusion of specific performance standards in Schedule 6 with which the Contractor must comply. The Committee believes that if a specific Year 2000 clause is not inserted in the agreement, it may be appropriate for Departments to address Year 2000 issues through specific performance standards in future contracts. The Contractor must also comply with any performance statements contained in the tender documentation.

The indemnity clause (clause 21) provides the following protection:

> *"The Contractor releases and indemnifies the Department and the State, their servants and agents from and against all damages, costs, expenses, loss or damage which they may incur or sustain and all actions, proceedings, claims and demands whatsoever which may be brought or made against them by any person, in respect of or by reason of or arising out of:*
>
> - *the provision of the Services (including project services) by or on behalf of the Contactor under this agreement;*
> - *any negligence or other wrongful act or omission of the Contractor or the Contractor's staff, employees or agents or of any other persons for whose acts or omissions the Contractor is vicariously liable;*
> - *any negligence or other wrongful act or omission of the Contractor's staff or the visitors, invitees or licensees of the Contractor;*
> - *death, injury, loss of or damage to the Contractor, the Contactor's staff or its other employees, agents, invitees, licensees or sub-contractors; and*
> - *any breach of this agreement by the Contractor."*

The Committee notes that this is a broad indemnity that attempts to cover the field in respect of potential liability. In the event of a Year 2000

problem, the key issue would be whether the failure of computer systems could be related back to the provision of particular services and the scope and specification of the services that were to be provided. For example, issues would include whether:

- the service provider was negligent in any way; or
- when the services were provided and the expected outcomes of the service.

These issues will need to be considered on a case by case basis and any Year 2000 issues directly addressed in the description of the services as provided in Schedule 2 – "Service Specification"

On the issue of solvency the Committee notes that the Contractor is required to obtain insurance pursuant to clause 22. This should be followed up by Departments as required in clause 22.4.

The Committee believes that this agreement only provides a minimum level of protection against the Year 2000 problem.

7.5 Year 2000 warranty

The Government's Year 2000 Policy issued in July 1996 requires all Departments to include the following clause in all "IT-based" contracts:

> *"The supplier warrants that insofar as the functioning or operation of any aspect of the product relies on, incorporates or otherwise utilises a date code:*
>
> - *the product has been specifically designed or adapted to accommodate and implement the transition from the twentieth century to the twenty first century;*
> - *a date occurring after 31 December 1999 shall be capable of being read and processed; and*
> - *where any step or process takes account of the difference between the two year numbers, the product is able to accurately compute such difference where one of those dates occurs in the twenty-first century and the other date occurs in the twentieth century."*

In addition the supplier is required to remedy any defect in the product which causes a breach of the warranty upon demand by the customer, whether or not such defect has resulted in a failure by the product at the time of the customer becoming aware of it. This obligation may be suspended if the customer receives a written assurance that an update or

replacement will rectify the problem and that update or replacement "will be available for implementation on a timely basis".

Finally, the supplier is required to indemnify the customer against all losses, claims, costs, demands and expenses which the customer may sustain as a result of the breach of the Year 2000 warranty.

The Committee has a number of concerns in relation to this warranty, including:

- it is not clear what an "IT-based contract" is. The Committee believes that the clause should be included wherever the Year 2000 may be a problem;
- it does not explicitly state that the product will continue to function; and
- it does not address the issue of interoperability, that is , where the software needs to operate with other applications.

The Committee recommends that:

Recommendation 7.1:	***All agencies review existing contracts with particular consideration to the following matters:*** • ***warranties that services and products are intended to function beyond 1999;*** • ***the drafting of specifications;*** • ***any exclusions or limitations on liability; and*** • ***indemnities.***

7.6 The GITC3 Year 2000 clauses

The GITC2 standard IT contract currently in use by the Government does not contain any specific reference to the Year 2000 problem. Departments are required to modify the GITC2 on a case by case basis to include a reference to Year 2000. The Committee was informed that most departments have not included the appropriate modifications to their IT service agreements.

The Office of Purchasing and Procurement (OPP) has advised the Committee that the GITC2 was to be replaced by the GITC3 in October 1998. The GITC3 includes a specific reference to Year 2000 as follows:

"Where the functioning or operation of any aspect of a Service or Product uses date/time data, the Contractor warrants that the service or product will:

- *comply with the Standards Australia standard SAA/SNZ MP77-1998 as amended from time to time; and*
- *be compatible with related products that will reference years until the end of 1999 by two or four digits if specified in the contract details."*

Essentially this clause requires the performance or functionality of any service or product to be maintained throughout the dates prior to, during and after the year 2000. The clause also requires the following compliance standards:

- no value for current date will cause any interruption in operation;
- date-based functionality must behave consistently for dates prior to, during and after Year 2000;
- in all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules; and
- year 2000 must be recognised as a leap year.

The product or service must also be able to operate with "related products".

The Committee is satisfied that the GITC3 clause clearly and explicitly covers the relevant Year 2000 issues and recommends its use by Departments in all relevant contracts, not just IT contracts.

The Committee recommends that:

Recommendation 7.2:	***Agencies include the GITC3 clause in all relevant contracts, not just IT contracts.***

7.7 Current government purchasing initiatives

The Committee was advised by the Office of Purchasing and Procurement[100] that the following initiatives to increase the level of protection afforded by current purchasing policies and guidelines in relation to the Year 2000 problem are planned:

- amendment to standard tendering documents and contracts;

[100] The Office of Purchasing and Procurement provides secretariat services to the Victorian Government Purchasing Board.

- establishment of a Website database and standard letter requesting data entries from all Government suppliers; and
- management of lead agency service panel contracts to ensure Year 2000 compliance.

Amendments to the standard form documents that were suggested by the OPP include the insertion of the following clause in all Government purchasing contracts:

> *"The successful tenderer is required to complete an entry in the VGPB Supplier Year 2000 Compliance Database (URL to be supplied) prior to execution of a contract. This entry will constitute a representation by the tenderer to the Victorian Government, which will be relied on, in the Victorian Government entering into the contract."*

The evaluation criteria for tendered services is also to be amended to include "demonstrated Year 2000 compliance" as a measure of the capability of a service provider. All service contracts will also include the GITC3 Year 2000 compliance standard as described above and the specifications for all contracts are to include the following clause:

> *"Please substantiate your Year 2000 compliance, as set out in the VGPB Supplier Year 2000 Compliance Database (insert URL) as part of your tender." [and if needed specify any particular Year 2000 technical requirements for this project]"* [101]

The Website initiative will allow government agencies to select suppliers from the VGPB Supplier Year 2000 Compliance Database. The suppliers on the Website database must have provided information in relation to the Year 2000 compliance of:

- the goods and services supplied to Government;
- their suppliers, who are critical to the ability to continue to supply government; and
- the supplier's business systems including equipment, plant and security systems.

The Committee was informed by the OPP that the vast majority (90 per cent) of the government's purchase contracts are the responsibility of the

[101] Quoted from documents tabled by the Office of Purchasing and Procurement at the PAEC private hearing, 11 September 1998.

Accredited Purchasing Units and that the above initiative will directly affect only 10 per cent of the contracts entered into by Departments.[102]

In these circumstances, the Committee remains concerned that agencies may not achieve the necessary protections offered by the new central purchasing arrangements.

The Committee recommends that:

Recommendation 7.3:	***The government immediately advise all government suppliers that year 2000 compliance is a requirement before they can enter into contract agreements with government agencies.***

Recommendation 7.4:	***Compulsory labelling of all IT equipment be introduced to indicate year 2000 compliance e.g. with the Standards Association of Australia/Standards New Zealand Year 2000 compliance standards.***

[102] PAEC private hearing, 11 September 1998.

Chapter 8: The Legal Implications of the Year 2000 Problem

"…no matter what sort of protection you give, some people are still not going to disclose information unless there is some other kind of legislative forcing of disclosure." [103]

8.1 Introduction

It is likely that the consequences of the Year 2000 problem will extend well into the next century and that the volume of resources devoted to its legal ramifications will be extensive. For example, it is estimated that insurance and legal claims worldwide will reach $US1 trillion.[104]

It is therefore essential that the government assesses the practical and social consequences of Year 2000 failure and develops adequate responses to avoid or minimise the risk of legal liabilities. The Committee believes it would be inappropriate to adopt a wait and see attitude.

As pointed out in Chapter 1, it is also necessary to recognise that the Year 2000 problem is not merely a computer problem. There will be legal ramifications for all stakeholders in Victoria's economy: businesses, government service providers, private individuals or groups of citizens, computer companies and IT consultants.

Reports by the NSW Audit Office and the Canadian Office of the Auditor-General state that the risks of litigation fall into the following classes:

- errors in government services and information on which businesses or the public rely;
- interruption in services that results in delays, causing loss of business;
- malfunction of products or devices certified by the government; and
- defects, errors, interruption or failure of goods or services regulated by the government.

Careful planning and remedial action may greatly reduce the likelihood that the government will either be a party to, or exposed to, litigation. Failure to address legal issues may lead to:

- loss of claims against vendors who otherwise might be required to pay for Year 2000 remediation costs;

[103] Ms Rebecca Davies, PAEC private hearing, 12 August 1998, p.2.

[104] Estimated by the Gartner Group, quoted from Merrill Lynch Australasia Report on the Year 2000 problem, July 1998. A trillion is $US1000 billion ($A1666 billion).

- delays from third party vendor lawsuits;
- legal liabilities for breach of contract, negligence, economic loss; and
- breach of statutory obligations.

It is essential that agencies identify:

- the legal liabilities that the Year 2000 problem create;
- where agencies are vulnerable to the Year 2000 problem, and assess the scope of their exposure; and
- a strategy plan, including processes for contract review and the identification of legal restraints.

To assist with the process, the following information identifies some of the legal issues and liabilities that the Year 2000 problem creates.

8.2 Overview of legal issues

Legal issues resulting from problems caused by Year 2000 failure could arise in a variety of contexts. These include legal actions in the following areas:

a) Providers of defective software

Where software fails to perform beyond one of the Year 2000 critical dates or fails to process information accurately, the supplier may be held legally liable for that failure. Liability will, however, depend upon a number of factors such as representations made regarding functionality, interoperability and compliance with specification. Failure to perform to specification may result in the software being classified as defective, possibly giving rise to an action for breach of warranty under the contract or pursuant to consumer protection laws such as the *Trade Practices Act* 1974 (Cth).

b) Suppliers of Year 2000 remediation services

Legal action may be taken against suppliers of Year 2000 services for the failure to adequately repair or modify software to deal with the Year 2000 problem. Software failure may result in the break down of operations of the primary business, which in turn may create consequential damage further down the chain of supply. This action may arise in a number of contexts such as negligence, breach of contract and liability under the *Trade Practices Act.*

Actions against outsourcers in tort (common law), contract or under the *Trade Practices Act* could be mounted for failure to detect, maintain and repair any problems relating to Year 2000.

c) Failure to disclose a Year 2000 problem

Actions may be taken against suppliers, contractors and others who failed to disclose a Year 2000 problem. For example, where a business is dependent upon another agency to maintain data or to provide services, non-disclosure or inadequate disclosure of a Year 2000 problem will mean that there is no capacity for the dependent business to avoid or minimise the risk of failure in that context. This may give rise to liability in tort and contract and pursuant to the *Trade Practices Act*. This applies to suppliers of goods and services, which are broadly defined. For example, the definition of "goods" in section 4 of the Act includes "gas and electricity".

d) Suppliers affected by Year 2000

Actions against suppliers affected by Year 2000 who cannot fulfil contractual obligations. This may give rise to an action in respect of breach of contract but may also leave the recipient party in breach of its own obligations and liable for a failure to perform.

e) Insurance claims

Actions may be brought against insurance companies for claims of coverage against the Year 2000 problem. Due to the foreseeable nature of the Year 2000 problem, however, it is questionable what level of insurance coverage for Year 2000 failure may be obtained. Older policies may provide some scope for argument, but many industries are now accepting that it will be impossible to obtain Year 2000 insurance.

The Committee received evidence from the CEO of the Year 2000 Industry Program[105] that Australia's peak insurance industry bodies were considering an announcement in 1999 of the general exclusion of Year 2000 from insurance coverage. Presently, however, insurance is still available to company directors who can substantiate Year 2000 compliance for their businesses.[106]

f) Indirect Year 2000 failures

Legal actions may be taken arising out of a failure that is indirectly due to a Year 2000 problem, for example, where contingency plans have not been developed or are inadequate. There is a great deal of scope for actions arising in tort and contract for consequential liability where a service is unable to be provided due to a failure further up the supply chain.

[105] PAEC, private hearing, 14 September 1998.
[106] *The Australian Financial Review*, 12 October 1998, Special Report, p.40.

g) Breach of a warranty

Actions may be taken against the providers of goods or services for breach of a warranty related to Year 2000 compliance (express or implied)**.** The *Trade Practices Act* contains a number of warranties regarding fitness for purpose and merchantability, which are implied under general consumer contracts. Liability in respect of the breach of such warranties will depend upon the precise terms of supply. For example:

- the purchaser of a product would need to have anticipated that it would continue to operate beyond 1999;
- there would need to be an ongoing obligation on the supplier to update and repair the product; and
- the nature of the product being supplied would need to be taken into consideration.

Suppliers of both software and computer hardware are affected by such warranties.

h) Service providers

Actions against service providers, including the government, could be taken by individuals or groups for the failure to provide a service due to Year 2000 failure. The key liability issue here would be negligence, although breach of contract may also be relevant.

i) Building owners

Legal action could be taken against employers or landlords for the failure to deal with Year 2000 issues arising in respect of key building equipment such as lifts, security and emergency warning systems and air-conditioning systems. In addition to actions in tort and contract (ie. pursuant to the lease), this may lead to liability under occupational health and safety legislation.

8.3 Legal liability

Liability in respect of Year 2000 failure can arise in a number of legal contexts. These include:

a) Directors' duties

Directors are required by the Corporations Law and the Australian Stock Exchange (ASX) reporting requirements to disclose information which is likely to have a material effect on the financial value of the company. In

1998 the ASX required listed companies to disclose their expenditures in addressing Year 2000 compliance.

Directors also owe a duty of care to the company to exercise the level of due care and skill that could be expected of a reasonable person in that position. This duty occurs at common law, in tort and equity, and pursuant to section 232 of the Corporations Law. The duty of care requires directors to adequately consider the Year 2000 problem and deal with it accordingly. This obligation may be affected by proposed changes to the Corporations Law to introduce a business judgement rule, although this is unlikely to dramatically alter the standard of care applicable in the circumstances.

b) Negligence

The law of negligence considers the behaviour of a reasonable person who is in a sufficiently proximate relationship with another person to owe them a duty of care in response to a foreseeable risk. If that duty is breached and results in loss or injury then the person will be liable.

The law looks at whether sufficient steps have been taken in response to a foreseeable risk. For example, it is reasonably well accepted that there is a general level of awareness of the Year 2000 problem, although the extent and accuracy of that understanding is open to question. It may be that failure of certain equipment or systems causing damage or injury to another person may be classified as a foreseeable risk. Certainly the failure to act in response to a known risk may fall below the standard expected of a reasonable person.

The Committee understands that findings of actual liability will depend upon the facts of individual cases and what was reasonable in particular circumstances. Due to these key questions of foreseeability and reasonableness, any court action on the issue of negligence is likely to be long, complex and expensive.

c) Contract

Actions in contract can only arise between parties who are in some form of pre-existing contractual relationship and the scope of the action will be determined by the nature of the contract itself which may deal with warranties, breach and remedies. An action may arise in respect of failure to comply with contractual terms and breach of express or implied warranties.

d) Consumer protection

The *Trade Practices Act* establishes certain standards for consumer protection, which are reinforced by State sale of goods and fair trading legislation. The *Trade Practices Act* contains a number of provisions that make manufacturers liable for personal injury caused by dangerous or defective goods. Section 75 (AD) provides that if a corporation supplies goods which it has manufactured and they have a defect and because of that defect an individual suffers injuries, the corporation is liable to compensate the individual.

Section 75AJ extends liability to the supplier where the consumer does not know who manufactured the goods and serves a notice on the supplier requesting details identifying the manufacturer. Where the supplier fails to provide details within thirty days they are deemed to be the manufacturer. Again this involves the assessment of whether the Year 2000 failure or malfunction may be deemed to be a defect within the meaning of the Act.

Liability may also arise under the general law of negligence. This may be of particular relevance to the supply of equipment containing embedded chips. In relation to misleading statements regarding Year 2000 compliance, regard should be had to section 52 of the *Trade Practices Act* which provides that a corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive. In addition to the general provisions of section 52 there are more specific provisions such as section 53. This means, for example, that where an agency claims that it or its products are Year 2000 compliant and ultimately they are found not to be compliant, it may be liable for misleading and deceptive conduct. For this purpose, it is irrelevant whether the statement was deliberately or inadvertently misleading.

e) Occupational health and safety

Employers are required by law to provide a safe system of work. The presence of embedded chips in a range of equipment and machinery gives rise to real concerns regarding how such equipment may function on and beyond critical dates. Areas of risk should be identified and dealt with as a matter of urgency, particularly where there is risk of personal injury. This may include security systems, air conditioning, lifts, time locks and warning devices.

Government, through its various departments and agencies, acts both as the supplier of services and products to the public and as a major recipient of goods and services provided by third parties. The government is therefore

involved at a number of levels in the chain of supply and has to consider a broad spectrum of liability issues.

The Committee recommends that:

Recommendation 8.1:	***Agencies review the potential Year 2000 failures that may affect their capacity to fulfil their contractual, community and legal obligations. Reviews should include an assessment of the impacts of any Year 2000 failures on suppliers of goods and services i.e. liability for failure on the part of the agency, and any organisation on whom the agency is dependent or inter-reliant.***

8.4 Cooperation and sharing of Year 2000 information

Given the limited period of time that remains it is essential that immediate steps are taken to deal with this problem. While many agencies have been working on the project for some time, others have made limited progress in identifying areas of risk. As the deadline approaches, it will be difficult to find sufficient personnel to remedy any problems that have been identified or which in fact may be materialising. It is therefore extremely important that any information and resources which are available are shared with as wide a group as possible.

The Committee believes that the sharing of information and resources will remove the need for agencies facing similar Year 2000 issues to reinvent the wheel, save time and money and hopefully ensure that the key systems are fixed prior to the critical dates. Several initiatives have been taken in both the private and public sectors for the sharing of Year 2000 information over the Internet. For example, Standards Australia and OGIT have web sites where Year 2000 compliant products can be registered and the Centre for Biomedical Engineering, Monash University, in partnership with the Department of Human Services, has a web site for the notification of Year 2000 related problems in biomedical equipment.[107]

However, the Committee is aware that there are widespread concerns that disclosure of Year 2000 information may expose the disclosing agency to

[107] Standards Australia – see *www.y2kregister.com.au;* OGIT - see *www.ogit.gov.au* and Centre for Biomedical Engineering – see *http://mucbey2k.eng.monash.edu.au/*. A list of over 129,000 Year 2000 compliant products is available at www.vendor2000.com.

liability on a number of levels. First, there is a concern that if an agency admits that it is not compliant, it will lose business and further, in the event of failure, this will be seen as an admission of liability. If it states that it is compliant and it turns out that it is not, it will be liable for misrepresentation, in tort and under State fair trading laws or the *Trade Practices Act.* A further complicating factor is that there appears to be no clear understanding of what compliance actually means.

Disclosure of information on a confidential basis may occur pursuant to a non-disclosure agreement but there is some concern that where such agreements are concluded amongst industry groups this may amount to anti-competitive conduct in breach of the *Trade Practices Act*. Section 45 of that Act provides that corporations shall not enter into contracts that in effect substantially lessen competition. It is arguable that an agreement between a group of competitors to disclose certain Year 2000 issues amongst themselves may have the effect of lessening competition. As the sharing of information and resources on this issue is highly desirable in the light of the tight timeframe, these concerns should be overcome by legislative clarification.

The Committee took evidence from a number of agencies and utilities that they would be willing to share information provided that any disclosure made regarding Year 2000 would not be used at a later stage as the basis for legal action. Other than certain Australian Stock Exchange reporting requirements, there is currently no legal obligation upon an agency to disclose its Year 2000 compliance status.

The Committee is aware that in the United Kingdom, cooperation and sharing of information on Year 2000 compliance is being encouraged by a voluntary system called Pledge 2000. This system calls on British businesses to sign a pledge that they:

- are actively working to minimise the impact of Year 2000 on their business;
- are committed to sharing information about resolving Year 2000 problems with those who have a genuine interest;
- will endeavour to provide accurate Year 2000 compliance information and assist customers to mitigate the impact of Year 2000 on existing products and services;
- will keep all Year 2000 information supplied to them confidential;
- will work cooperatively and in good faith with their supply chain partners on Year 2000 issues; and

- are working to solve the Year 2000 problem rather than taking legal action.

The Committee understands that this pledge does not create any legal obligations and is a non-binding statement of future intentions. Therefore it is nothing more than a goodwill gesture with no legal force.[108]

8.5 Good Samaritan legislation

In the United States, three bills known as Good Samaritan legislation have recently been considered by the US Congress. The legislation is intended to remove legal barriers to the disclosure of Year 2000 information and encourage the frank dissemination of information regarding Year 2000 preparedness. These Bills, described in the following sections, are:

- Year 2000 Liability and Antitrust Reform Bill;
- Year 2000 Information Disclosure Bill; and
- Year 2000 Information and Readiness Disclosure Act.

The US Senate and the House of Representatives both unanimously passed the third Bill, the *Year 2000 Information and Readiness Disclosure Act*, without debate on 26 September 1998 and on 29 September 1998, respectively. This Act encourages the exchange of information between businesses on compliance, tools and solutions to the Year 2000 problem. The Act also provides limited liability and evidentiary protection for those statements and disclosures.[109]

a) Year 2000 Liability and Antitrust Reform Bill

This Bill is intended to encourage the disclosure and dissemination of information about any steps taken to remedy the Year 2000 problem. It also provides an incentive for those involved in the computing industry and others to attempt to provide a remedy for any Year 2000 problems to the consumer by providing a limitation upon liability. The limitation applies to specific circumstances where a repair or replacement is made available to the customer or where all reasonable efforts have been made to protect against Year 2000 failure.

[108] Fewer than 100 UK companies have signed The Pledge, *The Australian*, 13 October 1998, p.53.

[109] Media release, "Year 2000 US Senate Passes Good Samaritan Legislation", Freehill, Hollingdale & Page, 1 October 1998. See also http://www.itaa.org and http://www.pli.edu. The President of the United States of America signed the Bill on 19 October 1998, *The Australian Financial Review*, 21 October 1998, p.46.

The Bill is divided into two sections, one dealing with the potential liability of computer software designers, developers and manufacturers for computer failure and the other dealing with the liability of other parties.

Where an action is brought against a developer, designer or manufacturer of computer systems, programs, software or components due to a computer date failure, the liability of that person is limited to an action based solely in contract (ie. it is excluding tort based liability) provided that:

- the plaintiff has not suffered any personal injury, other than emotional harm;
- the defendant has given notice by mail to all known purchasers of the computer system (or any component of the system) or software or hardware, that the system or product experiences or may experience a computer date failure and, with respect to buyers not known to the defendant, has given similar notice on the Internet;
- in relation to a computer product first introduced for sale after 31 December 1994, which was involved in the computer date failure, the defendant has made available at no charge a repair or replacement for that computer product; and
- in relation to a computer product first introduced for sale before 1 January 1995, which was involved in a computer date failure, the defendant has made a repair or replacement for that computer product available to the purchaser.

A distinction has been drawn between computer products available pre-and post 1995 in terms of cost of replacement products to the purchaser. This suggests that the purchaser is deemed to have accepted some of the risk of failure in relation to older computer products.

The notice to purchasers must contain details of the particular system or component of the system that experiences or may experience a computer date failure. It must also explain the manner in which the buyer can obtain a repair or replacement of the affected system (if available) or where they can obtain additional information.

The second section, dealing with liability of persons other than those involved in the computer hardware and software design, development and manufacturing industry, also includes steps for the limitation of liability. It provides that any action brought in relation to a computer date failure shall be deemed to be based solely in contract and will permit only the recovery of consequential business loss and the costs of repair or replacement resulting from the failure. This limitation will only operate where:

- the plaintiff has not suffered any personal injury other than emotional harm;
- the defendant has made all reasonable efforts to protect its system, program or software from a computer date failure, including efforts to acquire hardware or software that will not experience a computer date failure;
- the defendant has tested its computer systems by simulating the transition to 1 January 2000 and making any other test that a reasonable person would believe necessary to prevent a computer date failure, by no later than 1 July 1999;
- by no later than 1 August 1999, has provided notice to its customers (and the Council on Year 2000 Conversion) on its efforts to avoid failure, including a general description of its compliance efforts, the results of the compliance tests and the likelihood that it will make transition to the Year 2000, without failure; and
- posted this notice prominently in its place of business for public review.

The Committee has reviewed this Bill and provides the following general comments.

In order to minimise exposure the relevant agency must have taken all reasonable efforts to protect its computer system or products including the acquisition of new hardware and software. It would be difficult to establish what would satisfy the requirement of all reasonable effort, which is presumably a subjective standard dependent upon the knowledge, experience and financial resources of the agency. It would be necessary for all efforts to be documented to satisfy this requirement.

Testing must have been completed by no later than 1 July 1999. This simply may not be possible for many businesses and government agencies. Furthermore, tests must specifically involve the simulation of a rollover to year 2000 and any other test that a reasonable person would believe necessary. Given the limitation on obtaining external assistance with the Year 2000 problem, this test may be hard to satisfy.

The provisions are clearly aimed at compelling businesses to make full disclosure of their Year 2000 status, with the encouragement being provided by the limitation of liability to contract only claims.

The definition of computer system is broad, encompassing electronic devices, embedded chips and electronic calculators that are not programmable.

The Bill also provides that any conduct designed to mitigate the risk of failure, including the entry into an agreement, will not violate the antitrust provisions during the period from the enactment of the Bill until 31 December 2001. Anti-trust provisions are similar to the anti-competition provisions in Australia's *Trade Practices Act*.

The restriction of liability to actions based in contract limits the range of potential plaintiffs as they must have some form of contractual relationship with the defendant and provides some limitation on the assessment of damages.

The Committee understands that it will not apply where someone has suffered personal injury as a result of Year 2000 failure.

None of these provisions are intended to limit the parties' ability to enter into separate contracts dealing with the liability issue. This means that if parties chose to deal with their respective liability on a different basis this is contemplated and permitted by the legislation.

b) Year 2000 Information Disclosure Bill

The purpose of this Bill is to "promote the free disclosure and exchange of information related to Year 2000 readiness and to lessen the burdens on interstate commerce by establishing certain uniform legal principles in connection with the disclosure and exchange of information related to Year 2000 readiness."

The Bill excludes liability in a civil action (except any action brought by a Federal or State or other public authority acting in a regulatory, supervisory or enforcement capacity) in respect of an allegedly false, inaccurate or misleading Year 2000 statement, except where the statement is material to the cause of action, and:

- the statement was made with knowledge that it was false, inaccurate or misleading or made with intent to mislead or deceive or was made with a grossly negligent failure to determine its accuracy; or
- where the statement is a re-publication of a statement regarding a third party, knowledge that the statement was false, inaccurate or misleading or without a disclosure that the statement was based on information provided by another party that has not been verified.

A Year 2000 statement is defined as any statement concerning:

- an assessment, projection or estimate regarding Year 2000 processing capabilities of any agency, product or service;

- plans, objectives or timetables for implementing or verifying Year 2000 processing capabilities of an agency, product or service; or
- test plans, test dates, test results or operational problems or solutions related to Year 2000 processing by products or services that incorporate or use certain products.

The Bill also deals with the consequences of posting notices regarding Year 2000 issues to an Internet Web site. The posting of a notice on the relevant agency's Year 2000 Web site is presumed to be an adequate mechanism for providing notice, **provided that** no clearly more effective method of notice is practicable. Clearly this is intended to encourage the full and free disclosure of information on the Web sites of all relevant agencies. It does not create a positive duty to provide information about Year 2000 processing.

The Bill also deals with defamation and trade disparagement claims. Where the claim relates to a Year 2000 statement, the maker of such a statement shall not be liable unless it is established that the statement was made with knowledge that the statement was false or with reckless disregard as to the truth of the statement. In dealing with the issue of defamation, the Bill goes further than the other two Bills before the US Congress. It provides a greater scope of comfort to the maker of the Year 2000 statement but it may go further than is necessary to encourage discussion of the problem for the mutual benefit of the parties.

The Bill states that no Year 2000 statement shall be interpreted or construed as an amendment or alteration to any written contract between the parties, unless it is expressly agreed by the parties or forms part of the making of the contract. This prevents the unilateral amendment of terms of a contract by the party making the Year 2000 statement confirming, for the avoidance of doubt, what the position would be in general law.

The Bill provides for the designation of requests for the voluntary provision of information relating to Year 2000 processing as Special Year 2000 Data Gathering Requests, which shall be prohibited from disclosure under Freedom of Information. Such information may not be used in any civil action by a Federal agency, however, the Bill does not preclude such information being obtained by other means and used in such an action.

The protection granted by the Bill does not apply to actions brought by consumers in relation to a statement made to consumers directly in connection with the sale of a consumer product. Such a provision would be appropriate for equivalent Australian legislation given the existing provisions of the *Trade Practices Act*.

The most important thing that should be noted about the proposed legislation is that it does not address the liability of an agency arising from failure of a system due to a Year 2000 problem. The legislation is basically concerned with facilitating information dissemination. In this regard it adopts a soft approach by attempting to remove any indeterminate liability regarding disclosure of Year 2000 information. The Committee notes that it does not go any further than this, creating no positive obligations of disclosure.

c) Year 2000 Information and Readiness Disclosure Act

This Bill was passed by the US Congress and enacted on the 19 October 1998. The Act is very similar to the Year 2000 Information Disclosure Bill, the key differences being the:

- definition of "Year 2000 Statement" is expanded to include any statement attesting to, providing an opinion on, reviewing or otherwise commenting on any Year 2000 statement and any other statement directly or indirectly relating to Year 2000 processing capabilities;
- reference to gross negligence has been excluded;
- concept of the Year 2000 Readiness Disclosure is added and defines any Year 2000 Statement identified on face value as a Year 2000 Readiness Disclosure;
- definition of "Maker", as in the maker of a disclosure is included;
- exclusion of liability in respect of Year 2000 statements. The Act provides that no Year 2000 Readiness Disclosure or any portion thereof shall be admissible in any relevant legal action unless it is established that the disclosure was material and it was made with knowledge that it was false and misleading or with an intent to deceive, or where it is a re-publication regarding a third party, there is no statement that it is re-publication and the maker has not verified the original statement;
- in relation to the Year 2000 Web site, the reference to "except as provided by contract" rather than "no clearly more efficient method of notice". This provides added certainty;
- no reference is made to defamation issues (see note in this regard in previous section); and
- a new clause 7 providing that written disclosure regarding Year 2000 readiness made prior to the effective date of the Act and after 1 January 1998 would otherwise satisfy the requirements of being a Year 2000 Statement may be denominated as a Year 2000 Readiness Disclosure within 90 days of enactment of the Act.

The Committee was advised that legislation requiring the compulsory disclosure of Year 2000 status information would assist in encouraging the sharing of information on the Year 2000 problem in the private sector. The Committee would prefer a regime of voluntary disclosures and the cooperative sharing of Year 2000 information between all parties, although the option of compulsory disclosure may become necessary in 1999.

Some concerns have been raised with the Committee that if Good Samaritan legislation were enacted by State, Territories and the Commonwealth Governments it would shift the focus of legal argument to whether parties making Year 2000 disclosures did so recklessly or with an intention to mislead or deceive. Therefore legal actions regarding Year 2000 statements would not be minimised or avoided but merely altered in their focus.

However after reviewing all evidence, the Committee is aware that addressing the Year 2000 problem in time will be a tremendous challenge for all levels of government.

As our Inquiry has identified, much remains to be completed. For example, survey results taken from a variety of sources during 1997 and 1998 indicate that:

- small business is the lynchpin of commerce and critical to supply chains and yet has made little progress in achieving Year 2000 compliance;[110]
- three-quarters of SMEs have done nothing to avoid the expected effects[111] and up to 90 per cent are not prepared for the effects of the Year 2000 problem;[112]
- surveys carried out by the ASX show that 50 per cent of companies have not begun to focus on the Year 2000 issue;[113]
- a survey by the CPA showed that 78 per cent of small businesses have not spent any money on the Year 2000 problem;[114]
- in March 1998 a Morgan and Banks survey showed that 54.5 per cent of companies were still non-compliant and an additional 15.2 per cent did not know about the Year 2000 problem;[115] and

[110] PKF questionnaire http://www.pkf.com.au/y2k, reported in *The Australian,* 20 April 1998, p.37.
[111] Australian Bankers Association survey of SMEs in *The Australian,* 28 April 1998, p.24.
[112] Institute of Chartered Accountants, *The Australian,* 16 June 1998, p.45.
[113] Mr Richard Humphrey, Managing Director ASX in *The Australian* 7 April 1998, pp.56-57.
[114] CPA Small Business Health Index, in *The Australian,* 27 April, 1998, p.35.
[115] *The Age* 30 March 1998, Business News, p.1.

- a survey by Arthur Andersen showed that 40 per cent of Australian companies do not see the Year 2000 problem as a threat to their businesses.[116]

To strengthen efforts to address the Year 2000 problem, the Committee supports the enactment of legislation that would promote the sharing of information.

The Committee recommends that:

Recommendation 8.2:	***The Victorian Government give urgent consideration to introducing Good Samaritan legislation in Victoria to encourage the dissemination of information regarding Year 2000 preparedness and compliance issues.***

Recommendation 8.3:	***The government introduce Good Samaritan legislation in isolation of a national approach, if necessary.***

Recommendation 8.4:	***The proposed Good Samaritan legislation should:*** • ***be clear that pooling of information on the Year 2000 problem does not constitute anti-competitive conduct under the provisions of the Trade Practices Act;*** • ***provide clear incentives for information disclosure through limiting legal liability arising on the basis of such disclosures;*** • ***establish clear principles for effective information disclosure; and*** • ***have broad coverage but not alter consumer protection laws.***

8.6 Copyright issues

Computer software is protected as a literary work under the provisions of the *Copyright Act* 1968 (Cth). Section 31 of the *Copyright Act* provides that any adaptation or modification to software is an exclusive right of the copyright owner. Therefore any modification of software necessary to

[116] *The Australian*, 13 October 1998, p.37.

make it Year 2000 compliant will require the permission of the software owner.

Generally the use of software is restricted to the terms of the licence pursuant to which it was originally supplied and any amendments to that licence. The Committee was advised that it is extremely rare for a software licence to contain a right to modify the program in any way even where this is to rectify errors in the program.

Any Year 2000 "fix" is likely to involve a modification to the software, whether by the licensee, the software owner or a third party. Even the use of patches distributed by third parties is likely to infringe the rights of the software owner unless permission to incorporate such fixes has been granted. Under section 36 *Copyright Act* any modification of the software by a third party may also result in the licensee being liable for authorising the infringement of copyright.

It is therefore necessary for public agencies to identify:

- all software currently in use;
- the ownership of the software; and
- the relevant licence agreements that apply to software.

It may not be possible or practical to wait for the software provider to remedy the Year 2000 problem because the software owner may be difficult to trace, have insufficient resources, not have a remedy or charge prohibitive fees. Where permission to modify the software has not been included in the original licence it will be necessary for agencies to obtain the permission of the copyright owner to modify the software.

Further complications occur where a third party assesses Year 2000 functionality of the software without the permission of the copyright owner. Such tests involve the reproduction of the software in breach of the rights of the copyright owner and possibly the terms of licence agreements, potentially voiding any warranties.

The Committee notes that the Copyright Law Review Committee[117] recommended that:

> *The making by a lawful user of a computer program of a reproduction or adaptation of the program to restore its intended functionality should not infringe copyright where a correctly*

[117] Copyright Law Review Committee (1995) *Computer Software Protection* Paragraph 10.75. The recommendation was not implemented as it was overtaken by a comprehensive review of the Copyright Act, currently in progress.

functioning version of the program is not available within a reasonable time at a normal commercial price.

This approach would be a reasonable basis for excluding copyright infringement where modifications are made solely to remedy a Year 2000 problem. The Committee notes, however, that this recommendation was restricted to the intended functionality of the program. Thus the application of the recommendation may depend upon whether the program was originally intended to function beyond 1999. It may be necessary to broaden the scope of the exception to apply to any form of Year 2000 remedy.

The Committee recommends that:

Recommendation 8.5:	***In terms of copyright issues, agencies take the following action:*** • ***all software currently in use be identified and the terms affecting its use be clarified;*** • ***identify software which has a Year 2000 problem;*** • ***identify copyright owners who offer to make their software Year 2000 compliant and the terms and conditions of the offer; and*** • ***the written permission of the copyright owner is sought where the copyright owner offers no solution and modification is needed.***

Recommendation 8.6:	***The Government makes representations to the Commonwealth Government for the urgent amendment of the Copyright Act to:*** • ***exclude the reproduction of a program solely for the purpose of assessing Year 2000 compliance from infringement; and*** • ***permit modifications to software to remedy a Year 2000 problem. This exception may be absolute or subject to a reasonableness requirement such as granting the copyright owner the right of first refusal of repair, on reasonable terms and within a reasonable time.***

8.7 Documenting Year 2000 activity

The Committee understands that from commencement to final implementation, an agency's Year 2000 project could span four to five years. The documentation of decisions and action is essential in the event that agencies become the subject of legal action, or if agencies initiate legal proceedings, as a result of Year 2000 related systems failure, product failure or data errors. Agencies may be required to provide documented evidence that appropriate action and due diligence was taken to mitigate foreseeable Year 2000 risks when pursuing claims against (or defending claims by) third parties.

Exhibit 26 shows the survey results of agencies that documented real life tests on converted IT systems.

Exhibit 26

AGENCIES DOCUMENTING REAL LIFE TESTS [118]

Public agency	*No. agencies conducted real life tests*	*Agencies documenting real life tests*	*%*	*Agencies not documenting real life tests*	*%*
Departments & budget sector	9	6	67	3	33
Public hospitals & ambulance	26	15	58	11	42
Universities & TAFEs	10	3	30	7	70
Municipal councils	12	4	33	8	67
Regional water authorities	8	4	50	4	50
Public bodies	22	9	41	13	59
Companies, trusts & joint ventures	5	4	80	1	20
Regional library corporations	2	2	100	0	0
Public cemeteries	1	0	0	1	100
Superannuation funds	0	0	0	0	0
Regional waste management groups	1	0	0	1	100
Total public sector	**96**	**47**	**49**	**49**	**51**

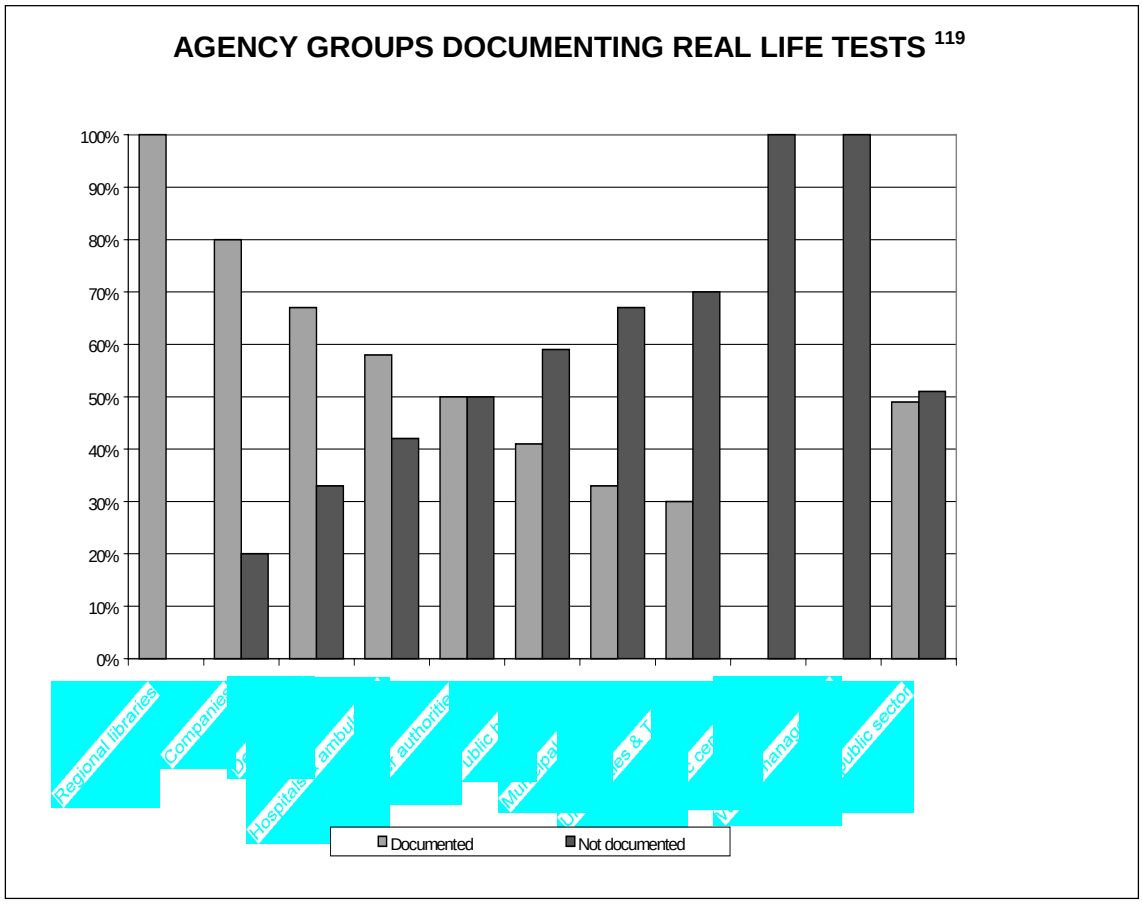
Exhibit 26 indicates that just over half of the agencies had failed to keep adequate records of the real life tests conducted.

Even in circumstances where real life tests have not produced date-related problems, the Committee believes that it is prudent for an agency to retain documented evidence of any tests conducted. In defence of any charges of negligence, agencies may need to produce documented evidence that due diligence or a duty of care had been fulfilled prior to the year 2000.

[118] Survey data for the period 3 March 1998 to 31 July 1998.

Exhibit 27 highlights the types of agencies that either have or have not retained documented evidence of real life compliance testing.

Exhibit 27



While it is pleasing that the majority of companies, Departments and hospitals had documented real life tests, the Committee is concerned to assure that all testing is properly documented.

The Committee recommends that:

Recommendation 8.7:	*The government ensure that all public sector managers are made aware of the legal liabilities of non-compliance.*

[119] Survey data for the period 3 March 1998 to 31 July 1998

The Committee recommends that *(continued):*

Recommendation 8.8:	***Agencies commence internal audits to identify potential areas where year 2000 liabilities may arise. The internal reviews identify potential year 2000 failures that may affect the government's capacity to fulfil its contractual, community and legal obligations.***

Recommendation 8.9:	***Internal reviews also include an assessment of the impacts of any year 2000 failures on persons who supply goods and services to government, ie. liability for failure on the part of the government and any organisation or dependent or inter-reliant entity.***

Recommendation 8.10:	***All agencies thoroughly document their year 2000 compliance activities to establish an audit trail to show that best efforts and due diligence had been taken.***

Recommendation 8.11:	***The government emphasise to all agencies the importance of retaining documented evidence of all year 2000 activities including all results of real life tests.***

Recommendation 8.12:	***Agencies develop strategies to protect against the occurrence of any identified liabilities.***

Recommendation 8.13:	***All agencies develop disaster recovery plans for business critical systems and that this be considered an aspect of any year 2000 disclosure legislation.***

Chapter 9: Community Assurances

"The businesses are concerned about public disclosure of information regarding their Year 2000 compliance programs because they recognise that issues of liability and litigation may arise if failures occur in practice. In dealing with the public disclosure issue an appropriate balance will have to be struck between the legitimate interests of the businesses involved and the public's need to know that appropriate actions are being taken to eliminate the risk of major failures" [120]

9.1 Introduction

The community faces an unknown risk that some critical services provided by governments and the private sector could be disrupted by the Year 2000 problem. Moreover, Victoria's infrastructure is a complex arrangement of public and private organisations with many interdependencies at all levels. These interdependencies among the Commonwealth, State and Local governments and within key economic sectors could cause a single failure to have adverse repercussions. Key economic sectors that could be seriously affected if their systems are not Year 2000 compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

Many witnesses reported that the Year 2000 readiness of the telecommunications sector is one of the most crucial concerns to Victoria because telecommunications are critical to the operations of nearly every public sector and private sector organisation.[121] For example, the information and telecommunications sector:

- enables the electronic transfer of funds;
- the distribution of electric power and the control of gas pipeline systems;
- is essential to the service economy, manufacturing and efficient delivery of raw materials and finished goods; and
- is basic to responsive emergency services.

Reliable telecommunications services are made possible by a complex web of highly interconnected networks supported by national and local carriers

[120] Dr John C. Tamblyn, Regulator-General, PAEC Private hearing, 21 August 1998, p.4.
[121] PAEC Private hearings, 28 August 1998; 10 September 1998, p.11.

and service providers, equipment manufacturers and suppliers and customers.

In addition to the risk associated with the State's key economic sectors, one of the largest, and largely unknown, risks relates to the global nature of the problem. With the advent of electronic communication and international commerce, Australia and the rest of the world have become critically dependent on computers. There are indications of Year 2000 problems in the international arena. For example, a June 1998 informal World Bank survey of foreign readiness found that only 18 of 127 countries (14 per cent) had a national Year 2000 program, 28 countries (22 per cent) reported working on the problem, and 16 countries (13 per cent) reported only awareness of the problem. No conclusive data were reported by the remaining 65 countries surveyed (51 per cent).

This highlights the severity of the problem and the important leadership role that the government has in:

- ensuring that there is a complete and accurate picture of Year 2000 progress;
- assessing the State's Year 2000 risks and setting State wide priorities;
- ensuring that critical systems, including those that impact directly on the community, are tackled first;
- ensuring the development and testing of contingency plans to maintain the continuity of critical public and private services; and
- promoting awareness of the Year 2000 problem within the community and the business sector and developing strategies with local government and industry groups that will address the risk areas.

The Committee believes that an important part of the government's Year 2000 strategy should be focused on the preparedness of the private sector and the community.

9.2. Preparedness of the private sector

While the terms of reference to this Inquiry restricted the Committee's scope to the Victorian public sector, evidence taken from a number of witnesses emphasised the interdependency of systems within the public and private sectors. The Committee was advised that while many larger companies had made significant progress in assessing and renovating critical systems, progress overall has been uneven across the private sector.

Most disturbing was the evidence that the 55,000 small to medium sized enterprises (SMEs) in Victoria are not taking the Year 2000 issue seriously

and that between 10 to 40 per cent of these small businesses may suffer interruptions in 2000.[122] The ripple effect, caused by the disruption to a number of interdependent supply chains, could lead to economic failures in other parts of Victoria's economy. The Committee believes this effect may impact on the community through the loss of jobs, disruption to food supply chains or the loss of vital government revenues and therefore services.

The Committee notes that the government has undertaken a number of initiatives to address the Year 2000 problem within the private sector, including an awareness raising campaign, the establishment of a support help line[123] and a Website.

The Committee believes that a great deal more needs to be done by the government to raise the awareness of SMEs of the Year 2000 problem and the need for appropriate contingency plans to ensure business continuity in 2000.

The other area of concern to the Committee relates to the Year 2000 compliance of companies that have interfacing business systems with government agencies. The government should develop a policy, which provides that agencies can only transfer electronic information with companies that have Year 2000 compliant computer systems. The Committee notes that such measures have been recently applied in other areas such as the banking and telecommunications industries.

9.3 Assurances for the community

As far as the Committee is aware, although all essential service organisations have contingency plans in place, the Government has not commenced planning for potential major disruptions to key services due to Year 2000 specific problems. For instance, the essential infrastructure utilities and emergency services gave evidence that they were unaware of each other's state of preparedness.[124] The Committee believes that the Government should develop a Year 2000 Public Confidence Program containing strategies on how to communicate key information about the compliance status of the essential services and the most probable impacts of the Year 2000 problem.

---

[122] From the State Government Small Business Victoria website http://www.sbv.vic.au/yr2000.htm, also reported in *The Herald-Sun*, 27 September 1998

[123] Inquiry service on 1800 11 2000 and Small Business Victoria website http://www.sbv.vic.au/yr2000.htm

[124] For example, at the various PAEC Private hearings for Telstra, VENCorp, Melbourne Water and the electricity industry.

To provide accountability to the Victorian public it is recommended that the Ministers primarily responsible for Year 2000 issues, report in the 1999 autumn and spring sessions to the Parliament on the status of critical projects and the strategies that are being developed to address key risk areas.

9.4 Performance against international best practice

ICA workshop participants developed the following guidelines and recommendations for managing the Year 2000 problem against which performance in the Victorian public sector can be measured:

- top management must take charge of the operation;
- government must take a lead;
- procedures for monitoring Year 2000 activities inside the public sector are required;
- methods for retaining key staff should be developed;
- budget implications and resource allocation procedures should be considered;
- the testing phase should not be underestimated;
- public sector buying power should be used to ensure cooperation and involvement from vendors;
- year 2000 compliance certificates should be agreed with suppliers; and
- coordination of standards for data interchange is required.

The Committee has assessed agency performance against the above guidelines. The following Exhibit indicates where the Committee believes the government needs to improve performance in relation to managing the Year 2000 problem:

Exhibit 28

PERFORMANCE ASSESSMENT

ICA Guidelines	Victorian Government practice
Top management must take charge of the operation.	Policy in place since July 1996 and at the direction of the Minister for Information and Technology and Multimedia. However, the response to the Year 2000 problem was mainly driven by IT managers at middle levels in Departments.[125] On 1 July 1998, a whole of government approach commenced with the establishment of the Year 2000 Risk Management Unit and a Cabinet accountability and reporting framework.
Government must take a lead.	Government needs to promote greater awareness of the issue for SMEs and the community sector. Government agency programs need to lead by example.
Procedures for monitoring Year 2000 activities inside the public sector are required.	In place since 31 August 1998 with the first Year 2000 status report to Cabinet by the Year 2000 Risk Management Unit. Greater auditing activity needed to ascertain status across critical areas.
Methods for retaining key staff should be developed.	To the Committee's knowledge there are no government initiatives to retain public sector IT staff.
Budget implications and resource allocation procedures should be considered.	As far as the Committee is aware, Year 2000 budgets are not set for the whole of government. In place for Departments and most agencies.
The testing phase should not be underestimated.	Testing may have been underestimated and it could be too late for some agencies given reluctance by major firms to start testing new systems in 1999.[126]
Public sector buying power should be used to ensure cooperation and involvement from vendors.	Currently in progress by the Victorian Government Purchasing Board. Should be in place in 1999. Not in place for IT purchases made since 1995.
Year 2000 compliance certificates should be agreed with suppliers.	Part of the Year 2000 policy. However, there was evidence that challenged the worth of Year 2000 compliance certificates.[127]
Coordination of standards for data interchange is required.	These issues have not been addressed at a whole of government level.

[125] Mr. Mike Harrington, Director, Special Projects Unit, Department of Premier and Cabinet, PAEC private hearing, 11 May 1998, p.1.

[126] For example, the major software company Oracle will not undertake any further Year 2000 consultancies in 1999 because it cannot guarantee all clients that there is enough time (i.e. at least 12 months) to complete testing for unforeseen problems, The *Australian*, 22 September 1998.

[127] For example, PAEC private hearings on 12 August 1998 and 28 August 1998 p.5, p.13.

9.5 Conclusion

Public sector respondent agencies have generally achieved best practice as measured against the ICA guidelines, however, the late start now warrants that the government give this issue a high priority. Resources must be directed towards the compliance of essential infrastructure services, hospitals, utilities and emergency services. All agencies need to prepare contingency plans to ensure at least minimum levels of service will be available in a worst case scenario.

The state government, local councils, industry and business groups and community groups all have a key role to play in preparing Victoria for the Year 2000 problem.

The Committee recommends that:

Recommendation 9.1:	***The government report by 31 January 1999 on the status of its objective for all business critical systems in the public sector to be compliant by 31 December 1998.***

Recommendation 9.2:	***The government ensure adequate resources are directed towards the compliance of essential infrastructure services, hospitals and the emergency services.***

Recommendation 9.3:	***The government promote greater awareness in SMEs of the Year 2000 problem and of the need for the development of appropriate contingency plans to ensure business continuity in the year 2000.***

Recommendation 9.4:	***The government advise local government and the Victorian community of the State's priority areas for year 2000 compliance.***

Recommendation 9.5:	***The government develop a Year 2000 Public Confidence Program containing strategies on how to communicate key information about the compliance status of community services and possible impacts.***

The Committee recommends that *(continued)*:

Recommendation 9.6:	***The government establish a Help Line and an organisational network of both public and private sector IT experts, which can provide assistance in the time leading up to the year 2000.***

Recommendation 9.7:	***The government establish a Community Contingency Planning Group through the Disaster Planning Organisation, the State Emergency Management Council, local councils and relevant community organisations, to plan for potential problems.***

Recommendation 9.8:	***The government establish by 30 November 1999 Communication and Incident Centres together with a year 2000 emergency call number.***

Recommendation 9.9:	***The government develop a year 2000 policy that provides that government agencies will not continue electronic business dealings with private sector companies that do not have year 2000 compliant computers.***

APPENDICES

Appendix 1

List of embedded chip devices with date-sensitive systems

Air circuit breakers
Air conditioning systems
Answering machines
Battery chargers
Building maintenance systems
Building security alarms
Cash registers
Closed circuit TV
Communication coupling modules
Communications
Compressed air systems
Continuous emissions monitoring systems
Controllers (PLCs, etc)
Converters
Conveyor control systems
Data acquisition systems
Data loggers
Data readers for electronic metering
Detectors
Diagnostic systems
Digital readouts
Distributed control systems
Electronic control systems
Electronic metering
Elevator controllers
Facilities management systems
Facsimile machines
Fire detection and protection
Flow meter/systems
Fuel card systems
Gas chromatographs
Gas metering
Generation units
Generator condition monitoring
Generator protection systems
Generator sets
Geological monitoring systems
Global positioning systems
Governors
Governors-generating sets
Industrial alarm systems
Manual handling equipment
Medical equipment
Meteorological equipment
MIL key systems
Mobile phones
Modems
Monitoring systems
Motor protection control
Network routers
PABX systems
Personal organisers
Personnel paging systems
Photocopiers
Photographic equipment
Postage franking machines
Radio communications
Reclosers
Recorders
SCADA (Supervisory Control and Data Acquisition system)
SCADA RTU
Security monitoring systems
Scientific calculators
Smart metering
Smart transmitters/positioners
Stacker/reclaimer PLCs
Stock control systems
Street lighting controls
Telephones
Time clocks/time recording systems
Timers
Traffic control systems
Uninterruptible power supplies
Variable speed drives
Vehicle engine management systems

Video cameras/recorders
Voicemail systems
Voltage regulators
Weight control systems
Wind speed and direction systems
Wind turbine controls
Word processing software

Source: Cobb, Dr. Adam (1998) 'Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks', Research Paper 18 1997-98, Foreign Affairs, Defence and Trade Group, 29 June 1998, Parliamentary Library, Parliament of Australia.

APPENDIX 2

LIST OF SUBMISSIONS

Alexandra District Hospital
Alpine Shire
Aluminium Smelters of Victoria Pty Ltd
Ambulance Service Victoria - South Eastern Region
Ambulance Service Victoria - North Eastern Region
Ambulance Service Victoria - North Western Region
Ambulance Service Victoria - South Western Region
Ambulance Service Victoria - Western Region
Anderson's Creek Cemetery Trust
Ararat Rural City Council
Architects Registration Board of Victoria
Austin and Repatriation Medical Centre
Australian Academy of Technological Sciences and Engineering
Australian Grand Prix Corporation
Australian Music Examination Board (Victoria) Ltd
Bacchus Marsh and Melton Memorial Hospital
Bairnsdale Regional Health Service
Ballaarat General Cemeteries
Ballarat Health Services
Banyule City Council
Barton Institute of TAFE
Barwon Region Water Authority
Bass Coast Shire Council
Baw Baw Shire Council
Beaufort and Skipton Health Service
Benalla and District Memorial Hospital
Bendigo Cemeteries Trust
Bendigo Health Care Group
Bethlehem Hospital
Board of Studies
Boort District Hospital
Borough of Queenscliffe
Box Hill Institute
Building Control Commission
Buloke Shire Council
Country Fire Authority
Cardinia Shire Council
Casey Institute of TAFE
Casey-Cardinia Library Corporation
Casterton Memorial Hospital
Central Gippsland Institute of TAFE
Central Highlands Water
Cheltenham Public Cemeteries Trust
Chiropodists Registration Board of Victoria
Cinemedia
City of Ballarat
City of Boroondara
City of Casey
City of Glen Eira
City of Greater Dandenong
City of Kingston
City of Melbourne
City of Monash
City of Moonee Valley
City of Wodonga
City West Water Limited
Cobram District Hospital
Cohuna District Hospital
Colac Community Health Services

List of Submissions (continued)

Coleraine District Hospital
Coliban Region Water Authority
Coopers and Lybrand
Council of Adult Education
Deakin University
Delatite Shire Council
Dental Board of Victoria
Dental Health Services Victoria
Department of Education
Department of Human Services
Department of Infrastructure
Department of Justice
Department of Natural Resources and Environment
Department of Premier and Cabinet
Department of State Development
Department of Treasury and Finance
East Gippsland Catchment Management Authority
East Gippsland Institute of TAFE
East Gippsland Shire Council
East Gippsland Water
East Grampians Health Service
Eastern Regional Waste Management Group
Echuca Regional Health
EcoRecycle Victoria
Emergency Services Superannuation Scheme
Energy Efficiency Victoria
Environment Protection Authority
Far East Gippsland Health and Support Service
Fawkner Crematorium and Memorial Park
First Mildura Irrigation Trust
Frankston City
Gannawarra Shire Council
Gas Services Business Pty Ltd
Gascor
Geelong Cemeteries Trust
Geelong Hospital
Geelong Performing Arts Centre
Geelong Regional Library Corporation
Gippsland Southern Health Service
Gippsland Water
Glenelg Shire Council
Glenelg Water Region Authority
Golden Plains Shire
Gordon Institute of TAFE
Goulburn Valley Base Hospital
Goulburn Valley Water
Goulburn-Murray Water
Grampians Region Water Authority
Greater Shepparton
Greyhound Racing Control Board
Hamilton Base Hospital
Harness Racing Victoria
Hepburn Health Service Inc
Hesse Rural Health Service
Heywood & District Memorial Hospital
High Country Library Corp
Hobsons Bay City Council
Holmesglen Institute of TAFE
Horsham Rural City Council
Hospitals Superannuation Board
Hume City Council
Hume-Moonee Valley Regional Library Corporation
Indigo Shire Council
Infertility Treatment Authority
Infrastructure Control Services
Inglewood and Districts Health Service
Inner and Eastern Healthcare Network
K P M G
Kangan Batman TAFE

List of Submissions (continued)

Keilor Cemetery
Kerang and District Hospital
Knox City Council
Kyabram and District Memorial Community Hospital
Kyneton District Health Service
La Trobe University
La Trobe University Union
Latrobe Regional Hospital
Legal Practice Board
Lilydale Memorial Park and Cemetery
Local Authorities Super
Loddon Shire Council
Lorne Community Hospital
Lower Murray Water
Macedon Ranges Shire Council
Maffra District Hospital
Maldon Hospital and Community Care
Mallee Track Health and Community Service
Manangatang and District Hospital
Manningham City Council
Mansfield District Hospital
Marine and Freshwater Resources Institute
Marine Board of Victoria
Maroondah City Council
Maryborough District Health Service
McIvor Health and Community Services
Melbourne 2006 Commonwealth Games Bid Pty Ltd
Melbourne City Link Authority
Melbourne Docklands
Melbourne Exhibition and Convention Trust
Melbourne Institute of Textiles
Melbourne Market Authority
Melbourne Port Corporation
Melbourne Research Enterprises Ltd
Melbourne Sports and Aquatic Centre
Melbourne Water
Memorial Park
Mental Health Review Board
Metropolitan Ambulance Service
Metropolitan Fire Brigades Board
Mildura Base Hospital
Mitchell Shire Council
Moira Shire Council
Montech Pty Ltd
Moreland City Council
Mt Alexander Hospital
Murray Valley Winegrape Industry Development Committee
Murrindindi Shire Council
Museum of Victoria
North East Region Water Authority
North Western Health Care Network
Northern Melbourne Institute of TAFE
Northern Regional Waste Management Group
Northern Victoria Fresh Tomato Industry Development Committee
Nurses Board of Victoria
O'Connell Family Centre (Grey Sisters) Incorporated
Office of Public Prosecutions Victoria
Office of the Regulator-General, Victoria
Omeo District Hospital
Outer Eastern Institute of TAFE Melbourne
Overseas Projects Corporation of Victoria Limited
Parks Victoria
Parliament of Victoria
Peninsula Health Care Network

List of Submissions (continued)

Peninsula Institute of TAFE
Plumbing Industry Board
Port Fairy Hospital
Portland and District Hospital
Portland Coast Region Water Authority
Prince Henry's Institute of Medical Research
Psychologists Registration Board of Victoria
Psychosurgery Review Board
Public Transport Corporation
Pyrenees Shire
Royal Melbourne Institute of Technology University
RMIT Innovation Ltd
RMIT Foundation
Robinvale District Health Services
Royal Botanic Gardens Melbourne
Rural Finance Corporation of Victoria
Seymour District Memorial Hospital
Shire of Melton
Shire of Strathbogie
Shrine of Remembrance Trustees
South East Water
South Eastern Waste Management Group
South Gippsland Hospital
South Gippsland Region Water Authority
South Gippsland Shire Council
Southern Grampians Shire
Southern Rural Water
St Arnaud District Hospital
St Vincent's Hospital Melbourne
State Library of Victoria
State Trustees
Stawell District Hospital
Stonnington City Council
Sunraysia Institute of TAFE
Sunraysia Rural Water Authority
Swan Hill District Hospital
Swan Hill Regional Library Corporation
Swan Hill Rural City Council
Tallangatta Hospital
Templestowe Cemetery and Memorial Gardens
Terang and Mortlake Health Service
The Beechworth Hospital
The Ian Potter Foundation
The Kilmore and District Hospital
The Necropolis
The Ombudsman
The Parliamentary Trustee
The Private Hospitals Association of Victoria
The Queen Elizabeth Centre
The Royal Melbourne Zoological Gardens
The Royal Women's Hospital
The School of Forestry Creswick Ltd
The University of Melbourne
Towong Shire Council
Transmission Pipelines Australia Pty Ltd
Treasury Corporation of Victoria
Tricontinental Corporation Limited
Trust for Nature (Victoria)
Tweddle Child and Family Service
University of Ballarat
Upper Murray Health and Community Services
Urban Land Corporation
Victoria University of Technology
VENCorp
Veterinary Practitioners Registration Board of Victoria
VicRoads (Roads Corporation)

List of Submissions (continued)

Victoria Legal Aid
Victoria Police Victorian Arts Centre Trust
Victorian Auditor-General's Office
Victorian Casino and Gaming Authority
Victorian Channels Authority
Victorian College of the Arts
Victorian Dairy Industry Authority
Victorian Electoral Commission
Victorian Financial Institutions Commission
Victorian Funds Management Corporation
Victorian Health Promotion Foundation
Victorian Institute of Forensic Medicine
Victorian Institute of Sport
Victorian Interpreting and Translating Services
Victorian Meat Authority
Victorian Plantations Corporation
Victorian Power Exchange Pty Ltd
Victorian Strawberry Industry Development Committee
Victorian Superannuation Board
Victorian Tertiary Admissions Centre
Victorian Workcover Authority
V/Line Freight Corporation
Wangaratta District Base Hospital
Warrnambool and District Base Hospital
Warrnambool City Council
Water Training Centre
Wellington Shire Council
Werribee Mercy Hospital
West Gippsland Healthcare Group
West Gippsland Regional Library Corporation
West Wimmera Health Service
Western Melbourne Institute of TAFE
Western Regional Waste Management Group
Western Water
Whitehorse Manningham Regional Library Corporation
Whittlesea City Council
Wimmera Health Care Group
Wimmera Mallee Water
Wodonga Institute of TAFE
Wodonga Regional Health Service
Wonthaggi and District Hospital
Yariambiack Shire Council
Yarra Valley Water
Yarram District Health Service
Yarrawonga District Hospital

Appendix 3

Letters sent to Ministers from the Committee

16 July 1998

Honourable Roger Hallam,
Minister for Finance and Minister for Gaming,
Level 3,
1 Treasury Place,
MELBOURNE VIC 3000

Dear Minister,

I understand that you have recently become responsible for whole-of-government issues relating to the Y2K problem.

Given the significance of the Year 2000 problem and its potential impact on the public sector and the community, earlier this year the Public Accounts and Estimates Committee appointed a Sub-Committee to undertake an inquiry into the Y2K issue and the level of preparedness of the public sector.

On 11 May, the Sub-Committee received a limited briefing on this matter from the Government Information Technology and Telecommunications Group and Mr Mike Harrington from the Department of Premier and Cabinet. At that time it was agreed that the Sub-Committee would receive further information after the matter had been considered by Cabinet. As Cabinet has now endorsed strategies relating to the management of the Year 2000 problem, I am writing to seek your support for the Sub-Committee to receive a further briefing on these initiatives.

If this proposal has your support, I suggest that officers of your department should liaise with the Committee's Executive Officer, Michele Cornwell, concerning the arrangements.

As the Committee is keen to report on this matter when the Parliament resumes in September, it would assist with expediting our Inquiry if we could receive the following information:

– the government's submission to our Inquiry (see attached letter dated 26 February 1998 – Attachment A);

– a response to the Committee's request for a copy of the Arthur Anderson report on the Year 2000 Plan Review (see attached letter dated 12 May 1998 -Attachment B); and
– a written reply to the attached list of questions (see Attachment C).

Your assistance in these matters would be appreciated.

Yours sincerely,

STEPHEN MCARTHUR
CHAIRMAN OF THE Y2K SUB-COMMITTEE

---

26 February 1998

Hon. Alan Stockdale, MLA
Minister for Multimedia
1 Treasury Place,
MELBOURNE VIC 3002

Dear Minister

INQUIRY INTO YEAR 2000 ISSUE: IS THE VICTORIAN PUBLIC SECTOR READY FOR THE MILLENIUM BUG?

In the 1997 Report on Ministerial Portfolios, the Auditor-General raised a number of concerns relating to the Year 2000 (Y2K) issue and the capacity of the Victorian public sector to address this situation.

Given the significance of this issue and the potential impact on the public sector, the Committee has resolved to examine the Y2K issue to:

- reinforce awareness of the significance of this issue and its potential impact across all levels of the Victorian public sector;
- analyse and assess the planning, risk management and coordination strategies adopted by the Victorian public sector to deal with this issue;
- assess the estimated total cost to the public sector of addressing this issue; and
- review the funding arrangements the Government has in place

- to ensure that its agencies and departments are Y2K compliant.

The concerns of the Committee fall into six categories:

- the costs involved and availability of resources to address the issue;
- contingency plans;
- service to the public;
- integrity of data bases;
- the role of Multimedia Victoria; and
- information for Parliament.

As Multimedia Victoria is responsible for the co-ordination of the Y2K issue in the Victorian Public Sector, the Committee would particularly welcome a submission on the following issues:

- From a whole of government perspective, what risks have been identified?
- From a whole of government perspective, what strategies have been developed to address these issues and what is the timetable for implementation?
- What activities are currently being undertaken across the Victorian public sector to ensure that all public sector entities will be Y2K compliant?
- What are the roles and responsibilities within and across government for addressing the Y2K problem?
- What are the total expected costs to the Victorian Government to address the issue?
- What are the funding arrangements for the resolution of the Y2K issue?
- What accountability mechanisms have been implemented by the government to assess the agencies' ability to effectively deal with the Y2K issue?
- Has consideration been given to requiring significant agencies/departments to provide certification to government once their systems are Y2K compliant?
- Has the government set a date by which it expects all public sector entities to be Y2K compliant?
- Has the government considered the legal implications of non-compliance? If so, what are the implications?
- Has the government issued a statement to agencies regarding the purchase of Y2K compliant products?
- Has consideration been given to developing an agreement between Federal and State Governments on the Y2K issue?
- What action has been taken to ensure the integration of the Y2K project with the implementation of IT outsourcing arrangements?

- What strategies have been developed to address:
- the limited availability of external consultants with Y2K expertise; and
- the limited number of IT staff with Y2K expertise in the public sector.

It would be appreciated if the Committee could receive your submission by **30 April 1998**.

To assist in determining the level of preparedness of the Victorian Public Sector to meet the challenges of the Y2K issue, the Committee will be undertaking a comprehensive survey of all agencies and departments. A copy of the questionnaire is attached.

Prior to the Sub-Committee holding public hearings on this issue, it would be appreciated if officers of Multimedia could provide a background briefing for Members.

Should officers of Multimedia Victoria require further information about this Inquiry they should contact the Executive Officer of the Committee, Michele Cornwell, ✆ 9651 3551.

Yours sincerely,

BILL FORWOOD
CHAIRMAN

Appendix 4

Private Hearings

List of organisations and witnesses who gave evidence at *in camera* hearings in Melbourne, Canberra and Sydney.

Private Hearings 11 May 1998

Department of Premier and Cabinet	Mr Mike Harrington, Director, Special Projects Unit
Multimedia Victoria	Mr Ian Webb, Director, Government Information Technology and Telecommunications Group
	Mr Randall Straw, Assistant Director, Information Technology
Advisor to the Committee	Professor Brian Garner, Professor of Computing Studies, Deakin University

Private Hearing 10 August 1998

Department of Treasury and Finance	Mr Adam Todhunter, Executive and Unit Director, Year 2000 Risk Management Unit

Private Hearings 12 August 1998

Year 2K National Steering Committee	Mr Graeme Inchley, Chief Executive Officer, Y2K Industry Program
Office of Information Technology	Mr Anthony Gates, Director Y2K Compliance
Australian Prudential Regulation Authority	Mr Graham Johnson, Chief Manager, Policy Development and Research
Reserve Bank of Australia	Mr Greg Johnston, Senior Manager, Payments System Stability, Payments Policy Department
	Mr Mike Hogan, Senior Manager, Policy and Administrative Systems, Systems and Technology Department

Private Hearings 12 August 1998 (continued)

Office of Government Technology	Mr Steve Fielding, Chairman of the Commonwealth/State Committee on Y2K
	Ms Glenys Roper, Chief Information Officer
Freehill, Hollingdale and Page	Ms Rebecca Davies, Partner

Private Hearing 21 August 1998

Office of the Regulator-General Victoria	Dr John Tamblyn, Regulator-General
	Mr Ian Wilson, General Manager

Private Hearings 28 August 1998

VENCorp	Mr Geoff White, Information Technology Manager
VicRoads	Mr Colin Jordan, Chief Executive
	Mr Doug Thompson, Director Finance
	Mr Geoff Kloot, General Manager, Traffic and Road Use Management
	Ms Susan Allen, General Manager, Registration and Licensing
	Mr John McNally, General Manager, Information Technology and Telecommunications
	Mr Peter Robinson, Executive Manager, Year 2000 Project
Gas Information Systems	Mr Neil Elliott, Chairman of Y2K Steering Committee for the Gas Industry and Chief Executive Officer, Kinetik Energy
	Mr Kevin Sharkey,Y2K Program Director for the Victorian Gas Industry
Melbourne Water	Ms Wendy Auchincloss, Information Manager

Private Hearings 10 September 1998

Electricity Industry	Mr Theo Van Der Meulen, SMS Consulting Group Pty Ltd
	Mr Greg Shedden, Manager IT Programs, United Energy
Department of Justice - portfolios of Victorian Police, Country Fire Authority, Metropolitan Fire and Emergency Services Board, and Victorian State Emergency Service	Mr John Charleson, Executive Director
	Ms Marisa De Cicco, Y2K Project Manager
	Mr Michael Tutchener, Y2K Project Manager
Department of Human Services	Mr Bob Reynolds, Assistant Director, IT Services
	Mr Jeff Supple, Manager Y2K Project
	Mr John Peoples, Assistant Director, Business Support and Project Development
Department of Infrastructure	Mr Jon Hickman, Deputy Secretary, Local Government, Planning and Market Information Services
	Mr Lyndon Thompson, Y2K Coordinator

Private Hearings 11 September 1998

Telstra Corporation	Ms Negba Weiss-Dolev, Group Director of the Year 2000 Program
	Ms Christine Johnston, National Manager, Customer Advocacy
Public Transport Corporation	Mr Andrew Neal, Chief Executive Officer
Department of Treasury and Finance	Mr Lance Bailey, Director of Purchasing and Procurement, VGPB Secretariat
	Mr Adam Todhunter, Executive Director, Year 2000 Risk Management Unit

Private Hearing 14 September 1998

Y2K Industry Program	Mr Graeme Inchley, Chief Executive Officer

Appendix 5

Survey Questionnaire

INQUIRY INTO THE YEAR 2000 PROBLEM: IS THE VICTORIAN PUBLIC SECTOR READY?

BACKGROUND

Given the significant of the Year 2000 (Y2K) issue and its potential impact on the Government's operations, the Public Accounts and Estimates Committee is undertaking a review to:

- assess the adequacy of agencies' planning in relation to achieving Y2K compliance; and
- reinforce awareness in the Parliament and the public and private sectors of the importance of various aspects of the Y2K problem.

INSTRUCTIONS

Please ensure that the questionnaire is:

- fully answered; and
- details of a suitable contact person are provided.

The Committee welcomes any written comments or explanations, which should be attached to the completed questionnaire.

The completed questionnaire should be returned by 30 April 1998 to:

Executive Officer
Public Accounts and Estimates Committee
8th Level
35 Spring Street
MELBOURNE VIC 3000
Phone: 03 9651 3551
Fax: 03 9651 3552
E-mail: paec@parliament.vic.gov.au

Further information about the Committee is available on the Internet at the following address:

http://www.vicnet.au/~paec

1. Please provide a breakdown of the number of computer systems in your agency including the number of servers and desktop computers.

   .....

1.1 Within each category how many of these are Y2K compliant?

   .....

1.2 How many of the systems, which are not Y2K compliant, are used in critical business activities?

   .....

1.3 Are all applications Y2K compliant? If not, please indicate the number of applications affected.

   .....

1.4 How many of the applications, which are not Y2K compliant, are used in critical business activities?

   .....

   If no computer systems or applications are affected by the Y2K problem, please return the questionnaire to the Committee following the completion of this question. Otherwise, please continue with question 2.

2. Please outline the major risks that the Y2K problem presents to your agency and to your clients?

   .....
   .....
   .....
   .....
   .....
   .....
   .....

3. Does your agency have a documented Y2K Compliance Program/Risk Management Plan?

   Yes ☐ No ☐

   If no, please provide an explanation why a compliance project has not been undertaken.

   .....
   .....
   .....
   .....
   .....

   If yes, please provide a copy of the plan to the Committee and continue with the remainder of the questionnaire.

4. What is the commencement date for the Y2K compliance program?

.....

5. Does the Y2K compliance program address all:

a) potential information technology (IT) exposure? Yes ☐ No ☐

b) non-IT exposure? (ie. card key systems, elevators, etc.) Yes ☐ No ☐

c) business services exposure? Yes ☐ No ☐

6. What is the compliance approach being taken by the agency for the computer systems?

Please tick the appropriate box.

☐ Replace many of the systems ☐ Modify them to be Y2K compliant

☐ Depends on the system ☐ Undecided at this point

☐ Outsource IT Operations ☐ Other (please describe)

7. Has a Y2K Task Force or group been established to address the issue?

If no, please proceed to question 11. Yes ☐ No ☐

8. How many people are included on the Task Force?

.....

9. Does the Task Force include both internal and external resources?

Yes ☐ No ☐

10. What resources and skills have been assigned to the Task Force?

……
……
……
……
……
……
……

11. Is your agency working with any of the vendors listed below on the Y2K issue? Please include any other types of vendors working on the Y2K issue for your agency.

- ☐ Hardware vendors
- ☐ System software vendors
- ☐ **Operational suppliers**
- ☐ **Other vendors**
- ☐ Application software vendors
- ☐ Consultants

……..
……..
……..

12. Please identify any of the external parties listed below with whom your agency is working with on the Y2K Issue. Also include any other external parties.

- ☐ Customers
- ☐ Banks and other financial institutions
- ☐ Government and regulatory agencies
- ☐ Electronic data interchange (EDI)

……..
……..
……..

13. What is the level of executive support for the Y2K program?

……
……
……

14. Has your agency commenced documenting the inventory of:

a) business services? Yes ☐ No ☐

b) IT products? Yes ☐ No ☐

c) Non-IT services? Yes ☐ No ☐

15. Has the business risk for inventoried systems been defined? Yes ☐ No ☐

16. Has a business risk rating been assigned to the various suites of applications?

Yes ☐ No ☐

17. Has your agency conducted Y2K "real life" compliance tests on:

a) major business functions? Yes ☐ No ☐

b) externally supplied IT products? Yes ☐ No ☐

c) internally supplied IT products? Yes ☐ No ☐

d) externally supplied Non-IT products? Yes ☐ No ☐

e) internally supplied Non-IT products? Yes ☐ No ☐

18. Are any of the above results of testing formally documented? Yes ☐ No ☐

19. Please indicate your current status in ensuring Y2K compliance?

☐ Planning Phase ☐ Assessment Phase

☐ Conversion Phase ☐ Implementation

20. How many applications are at each stage of the Y2K compliance process

Compliant: .....
In process: .....
Planned: .....
No plans: .....
Do not need to be compliant: .....
Other: .....

21. Have critical milestones been established to indicate that current initiatives are on target? Yes ☐ No ☐

22. Is the agency's Y2K compliance program on schedule? Yes ☐ No ☐

If no, explain the complications faced by the agency:

……
……
……
……
……
……
……

23. When will the agency be Y2K compliant?

……..

24. Have contingency plans been established to mitigate the risks associated with the program not being completed on time?

Yes ☐ No ☐

If yes, please describe:

……..
……..
……..
……..
……..
……..
……..
……..
……..
……..

25. What is the agency's estimate of the total cost to become Y2K compliant?

……..

26. Based on your agency's Y2K activities since its inception, how much has been spent, by year and amount, exclusively by your agency's Y2K project?

……..
……..
……..
……..
……..
……..

General Questions

27. Are further improvements required in the overall co-ordination of the Y2K compliance issue?

……..
……..
……..
……..
……..
……..

28. What strategies have been developed to address the limited number of:
    a) IT staff with Y2K expertise? and
    b) IT consultants with Y2K expertise?

    ……
    ……
    ……
    ……
    ……
    ……

29. Are there any other comments you wish to make?

    ……
    ……
    ……
    ……
    ……
    ……

Contact Officer

Name .....

Position .....

Contact No .....

Appendix 6

List of inner and outer budget agencies who responded to the Committee's Questionnaire

Departments and other independent budget sector agencies

Department of Education
Environment Protection Authority
Department of Human Services
Department of Infrastructure
Department of Justice
Department of Natural Resources and the Environment
Office of the Ombudsman
Office of the Chief Commissioner of Police
Department of the Premier and Cabinet (*refers to the Department of Treasury and Finance response*)
Office of the Director of Public Prosecutions
Office of the Public Service Commissioner, (*refers to the Department of Premier and Cabinet response*)
Office of the Regulator-General
Department of State Development
Department of Treasury and Finance
Victorian Auditor-General's Office
Victorian Electoral Commission

Public bodies

Architects Registration Board of Victoria
Australian Grand Prix Corporation
Board of Studies
Building Control Commission
Chiropodists Registration Board of Victoria
Cinemedia Corporation
Council of Adult Education
Country Fire Authority
Dental Board of Victoria
Docklands Authority
Eco Recycle Victoria
GASCOR
Geelong Performing Arts Centre Trust
Harness Racing Board
Heritage Council (*refers to Department of Infrastructure response*)
Infertility Treatment Authority
Legal Practice Board
Liquor Licensing Commission (*refers to Department of State Development response*)
Marine and Freshwater Resources Institute
Marine Board of Victoria
Melbourne City Link Authority
Melbourne Market Authority
Melbourne Port Corporation
Melbourne Water Corporation
Metropolitan Fire Brigades Board
Murray Valley Citrus Marketing Board
Museums Board of Victoria
National Police Ethnic Advisory Bureau (*refers Office of the Chief Commissioner of Police response*)
Northern Victorian Fresh Tomato Industry Development Committee
Nurses Board of Victoria
Office of Gas Safety *(refers to VENCorp response*)

Parks Victoria
Plumbing Industry Board
Prince Henry's Institute of Medical Research
Psychologists Registration Board of Victoria
Psychosurgery Review Board
Public Transport Corporation
Roads Corporation
Royal Botanic Gardens Board
Rural Finance Corporation of Victoria
Shrine of Remembrance Trustees
State Library of Victoria Foundation
Tourism Victoria (*refers to Department of State Development response*)
Treasury Corporation of Victoria
Trust for Nature (Victoria)
Urban Land Corporation
VENCorp
Veterinary Practitioners Registrations Board of Victoria
Victoria Legal Aid
Victorian Casino and Gaming Authority
Victorian Channels Authority
Victorian Dairy Industry Authority
Victorian Financial Institutions Commission
Victorian Funds Management Corporation
Victorian Health Promotion Foundation
Victorian Institute of Forensic Medicine
Victorian Interpreting and Translation Service
Victorian Meat Authority
Victorian Plantations Corporation
Victorian Power Exchange
Victorian Strawberry Industry Development Committee
Victorian Tertiary Admissions Centre
Victorian Workcover Authority
V/Line Freight Corporation
Water Training Centre
Zoological Parks and Gardens Board

Universities and other educational institutions

Barton Institute of TAFE
Box Hill Institute of TAFE
Casey Institute of TAFE
Central Gippsland Institute of TAFE
Deakin University
East Gippsland Institute of TAFE
Eastern College of TAFE
Gordon Institute of TAFE
Holmesglen Institute of TAFE
Ian Potter Foundation (*refers to The University of Melbourne response*)
Kangan Batman Institute of TAFE
La Trobe University
Melbourne Institute of Textiles
Northern Melbourne Institute of TAFE
Peninsula Institute of TAFE
Royal Melbourne Institute of Technology
Sunraysia Institute of TAFE
The School of Forestry, Creswick Ltd
The University of Melbourne
University of Ballarat
Victoria University of Technology
Victorian College of the Arts
Western Melbourne Institute of TAFE
Wimmera Institute of TAFE (*refers to University of Ballarat response*)
Wodonga Institute of TAFE

Public cemeteries

Anderson's Creek Cemetery Trust
Ballarat General Cemeteries Trust
Bendigo Cemeteries Trust
Cheltenham and Regional Cemeteries Trust
Geelong Cemeteries Trust
Keilor Cemetery Trust
Templestowe Cemetery Trust
Trustees of the Fawkner Crematorium and Memorial Park
Trustees of the Lilydale Memorial Park and Cemetery
Trustees of the Memorial Park Altona
Trustees of the Necropolis Springvale

Public hospitals and ambulance services

Alexandra District Hospital
Ambulance Services Victoria -
Metropolitan Region
North Eastern Region
North Western Region
South Eastern Region
South Western Region
Western Region
Austin and Repatriation Medical Centre
Bacchus Marsh and Melton Hospital
Bairnsdale Regional Health Service
Ballarat Health Services
Barwon Health
Beaufort and Skipton Health Service
Beechworth Hospital, The
Benalla and District Memorial Hospital
Bendigo Health Care Group
Bethlehem Hospital Incorporated.
Boort District Hospital
Caritas Christi Hospice Ltd (*refers to St Vincent's Hospital's response*)
Casterton Memorial Hospital
Cobram District Hospital
Cohuna District Hospital
Coleraine and District Hospital
Dental Health Services Victoria
East Grampians Health Service
Echuca Regional Health
Far East Gippsland Health and Support Service
Geelong Hospital
Gippsland Southern Health Service
Goulburn Valley Base Hospital
Hepburn Health Service
Hesse Rural Health Service
Heywood and District Memorial Hospital
Inglewood and District Health Service
Kerang and District Hospital
Kilmore and District Hospital
Kyabram and District Memorial Community Hospital
Kyneton District Health Service
Latrobe Regional Hospital
Lorne Community Hospital
Maffra District Hospital
Maldon Hospital
Mallee Track Health and Community Service
Manangatang and District Hospital
Mansfield District Hospital
Maryborough District Health Service
McIvor Health and Community Services
Mercy Public Hospitals Inc. (Werribee Campus)
Mildura Base Hospital
Mount Alexander Hospital
North Western Health Care Network

O'Connell Family Centre (Grey Sisters) Inc.
Omeo District Hospital
Peninsula Health Care Network
Port Fairy Hospital
Portland and District Hospital
Queen Elizabeth Centre
Robinvale District Hospital and Health Services
Seymour District Memorial Hospital
St. Arnaud Hospital
St Vincent's Hospital (Melbourne) Ltd
Stawell District Hospital
Swan Hill District Hospital
Tallangatta Hospital
Terang and Mortlake Health Services
Tweddle Child and Family Health Service
Upper Murray Health and Community Services
Wangaratta District Base Hospital
West Gippsland Health Care Group
West Wimmera Health Service
Wimmera Health Care Group
Wodonga District Hospital
Women's and Children Health Care Network
Wonthaggi and District Hospital
Yarram and District Health Service
Yarrawonga District Hospital

Superannuation funds

Coal Mine Workers' Pension Fund (*refers to Victorian Superannuation Board response*)
Emergency Services Superannuation Board
Hospitals Superannuation Board
Local Authorities Superannuation Board
State Superannuation Fund (*refers to Victorian Superannuation Board response*)
Victorian Superannuation Board
Victorian Superannuation Fund (*refers to Victorian Superannuation Board response*)

Companies, trusts and joint ventures

Aluminium Smelters of Victoria Pty Ltd (t/as Aluvic)
Australian Music Examinations Board (Vic.) Ltd
City West Water Ltd
Gas Services Business Pty Ltd
La Trobe University Union
Melbourne Convention and Exhibition Trust
Melbourne Research Enterprises Ltd
Melbourne Sports and Aquatic Centre Trust
Melbourne 2006 Commonwealth Games Bid Pty Ltd
Monash IVF Pathology Services Trust
Monash IVF Pty Ltd
Montech Pty Ltd
Overseas Projects Corporation of Victoria Ltd
RMIT Foundation
State Trustees Limited
Transmission Pipelines Australia Pty Ltd
Tricontinental Corporation Ltd
Victorian Arts Centre Trust
Victorian Institute of Sport Ltd
Yarra Valley Water Ltd

Water authorities

Barwon Region Water Authority
Central Highlands Region Water Authority
Coliban Region Water Authority
East Gippsland Catchment Management Authority
East Gippsland Water
First Mildura Irrigation Trust
Gippsland Water
Glenelg Region Water Authority
Goulburn-Murray Water
Goulburn Valley Water
Grampians Region Water Authority
Lower Murray Water
North East Region Water Authority
Portland Coast Region Water Authority
South Gippsland Region Water Authority
Southern Rural Water
Sunraysia Rural Water Authority
Western Water
Wimmera-Mallee Water

Regional waste management groups

Eastern Regional Waste Management Group (t/as LEAST)
Northern Regional Waste Management Group
South Eastern Regional Waste Management Group
Western Regional Waste Management Group

Municipal councils

Ararat Rural City Council
Ballarat City Council
Banyule City Council
Bass Coast Shire Council
Baw Baw Shire Council
Boroondara City Council
Buloke Shire Council
Cardinia Shire Council
Casey City Council
Delatite Shire Council
East Gippsland Shire Council
Frankston City Council
Gannawara Shire Council
Glen Eira City Council
Glenelg Shire Council
Golden Plains Shire Council
Greater Dandenong City Council
Greater Shepparton City Council
Hobsons Bay City Council
Horsham Rural City Council
Hume City Council
Indigo Shire Council
Kingston City Council
Knox City Council
Loddon Shire Council
Macedon Ranges Shire Council
Manningham City Council
Maroondah City Council
Melbourne City Council
Melton Shire Council
Mitchell Shire Council
Moira Shire Council
Monash City Council
Moonee Valley City Council
Moreland City Council
Murrindindi Shire Council
Pyrenees Shire Council
Southern Grampians Shire Council
Stonnington City Council
Strathbogie Shire Council
Swan Hill Rural City Council
Towong Shire Council
Warrnambool City Council
Wellington Shire Council
Whittlesea City Council
Wodonga Rural City Council
Yarriambiack Shire Council

Regional libraries corporations

Casey-Cardinia Regional Library Corp.
High Country Regional Library Corp.
Hume-Moonee Valley Regional Library Corp.
Swan Hill Regional Library Corp.
West Gippsland Regional Library Corp.
Whitehorse Manningham Regional Library Corp.

Appendix 7

Victorian Government Year 2000 Policy (issued July 1996)

Policy

Departments should plan, resource and implement procedures to ensure that computer-based information systems will correctly process dates with a century-20 component.

Background

With the year 2000 approaching, and within the processing horizon of computer-based information systems, significant date-processing problems are anticipated in both hardware and software. Many systems have a critical dependence on the absolute correctness of date-processing.
Traditionally, most application systems have adopted a Gregorian date format and truncated the year component to the two least-significant digits, which represent the decade. Period-calculating routines which use decade-digits as an argument will fail, and editing routines, particularly for input data, will, in all probability, reject '00'. Vendor provided software, including operating systems, is not immune.
Due to the wide variety of information technology hardware, software and applications deployed within the Victorian public sector there is no single, nor simple, solution to the problem. Three major issues clearly emerge from experiences with the issue -

i) Cost of Conversion - Authoritative estimates indicate that substantial cost is involved in identifying, locating and re-programming date-processing routines. Additionally, the establishment of testing environments and the conduct of modification testing are potentially significant cost items;
ii) Time Available - The problem horizon is not negotiable. At best, some three years remain for corrective action. At worst, in those systems that process future-dates, the problem will occur earlier than 1 January 2000; and
iii) Workload - The USA experience in addressing this problem has been a significant IT workload increase coupled with the need for expert local systems knowledge.

Implementation Guidelines

As the resources of every department will be effected by this problem, it is imperative that work commence immediately to address the size of the problem. The deployment of many different IT architectures across the budget-sector make a definitive or prescriptive approach inappropriate. These guidelines are provided to assist departmental planners. Practitioners should be mindful that there is the potential for this problem to occur in all software (operating systems, off-the-shelf and bespoke applications) and some hardware.

Scope and Size of the Problem

What systems are -

- date-processing dependent?
- dependent upon forward date-processing?
- dependent upon internal/external date transfers/interfaces?
- critical to core business?
- expected to be operational within the problem-window?
- under construction or consideration?

Workload Estimation

Whilst each department is ultimately responsible for the problem resolution, who is responsible for carrying out the actual work? Is it the product vendor, an outsourcing contractor or an internal responsibility?
If internal, what effort is required to -

- identify and locate the date-processing code in each system?
- check the date-processing code for correctness?
- rectify problems found? and
- test modifications?

If vendor products, will the vendor assume responsibility for the effort and cost of the correction process including testing?
If outsourcing contractor, is the situation covered by existing contractual arrangements or will a new set of conditions need to be negotiated?

Implementation Process

The major issues are how, where and when will be work be performed?

How will the work be carried out?

- will a co-ordinated effort be mounted and managed across the portfolio?

- will internal/external resources be used and have they been budgeted ?
- are manual/automated correction methods available and appropriate?

Where will the work be carried out?

- has the present IT architecture the capacity to handle the additional load?
- can a system copy be shipped to an alternative site for corrective work?

When will the work be carried out?

- can the corrective work be performed during normal business hours?
- has the system critical dates to avoid, e.g., end of financial year?

Additionally, all IT-based contracts should contain conditions that address this issue. A suggest form is -

Year 2000 Warranty

Clause X.1 [The Supplier] warrants that insofar as the functioning or operation of any aspect of the product relies on, incorporates or otherwise utilises a date code:

a) the product has been specifically designed or adapted to accommodate and implement the transition from the twentieth century to the twenty-first century;
b) a date occurring after 31 December 1999 shall be capable of being read and processed; and
c) where any step or process takes account of the difference between two year numbers, the product is able to accurately compute such difference where one of those dates occurs in the twenty-first century and the other date occurs in the twentieth century.

Clause X.2 Notwithstanding that this agreement or any warranty provision in it is expressed to endure for a period of time, the warranty provided for in sub-clause 1 shall survive termination of this agreement and shall endure for the life of the product.

Clause X.3 [The Supplier] shall immediately on demand by the [Customer] remedy or correct any defect in the product which causes a breach of the warranty in sub-clause 1 whether or not such defect has resulted in a failure by the product at the time of the [Customer] becoming aware of it.

Clause X.4 [The Supplier's] obligation to comply with sub-clause 3 may be suspended by the [Customer] in its absolute discretion if the [Customer] receives written assurances from the [Supplier] that an update, new release, new version or replacement will rectify such defect and that such update, new release, new version or part will be available for implementation on a timely basis.

Clause X.5 [The Supplier] shall indemnify, keep indemnified and hold the [Customer] harmless against all losses, claims, costs, demands and expenses whatsoever and howsoever arising which the [Customer] may sustain or incur as a result of a breach of the warranty in sub-clause 1.

Clause X.6 For the purposes of this clause, "product" means program/software/hardware/system/firmware/source code/object code as the case requires.

Other Relevant Information

This subject has attracted attention world-wide and generated a considerable amount of literature. Some of the more useful material relates to the testing of specific software products for year-2000 processing. A wide range of starter-material can be found on the Internet sites -

http://www.year2000.com/

IT Policy will be seeking, and suggesting, amendments to the Government Information Technology Conditions (GITC) Version 2. If, and until, changes are made to the GITC the suggested conditions may be obtained by contacting Randall Straw - Email: randall.straw@mmv.vic.gov.au

Appendix 8

Year 2000 Annual Reporting Requirements (issued July 1998)

9.6 Year 2000 Compliance Requirements and Disclosures[128]

9.6.1 Background

Many date-dependent electronic control systems, including computerised information, process and access control systems, were developed using a two-digit field for the year. When the century changes on 1 January 2000 systems may malfunction due to their inability to correctly process "00" and therefore systems will need to be addressed and remedied where necessary, before 1 January 2000.

The Australian Stock Exchange Limited has adopted a uniform standard for Year 2000 compliance issued by the Standards Association of Australia and New Zealand (SAA/SNZ MP77:1998). The standard has been adopted as an accepted benchmark for assessing achievement of compliance by departments and public bodies in the Victorian public sector and forms the basis for reporting under Direction 9.1.2. The Guidelines below adopt an approach to compliance reporting which is similar to the recommendations of the Australian Stock Exchange and so maintain consistency of reporting standards between two sectors of the Victorian economy.

The Government requires that all reporting entities include in their annual reports to Parliament a statement of progress towards Year 2000 compliance by listing all classes of 'business-critical systems' in use and the scheduled dates by which those systems will be Year 2000 compliant.

9.6.2 Directions

(i) Relevant financial and other information in respect to a financial year should include a statement of progress towards Year 2000 compliance by listing all classes of 'business-critical systems' in use and the scheduled dates by which those systems will be Year 2000 compliance

(ii) "Business-critical" means: Information technology-based systems (software, hardware and data communication links, including embedded chip technology, such as monitoring, dispensing and telemetry systems) whose sudden, temporary or permanent

[128] **Source**: *Part 9 of the Directions of the Minister for Finance, 30 July 1998*

unavailability or unreliability would compromise the quality, quantity or timing of their service delivery and includes systems associated with:

- health and safety
- community security
- emergency services
- utility services
- revenue collection and distribution

(iii) Compliance is to be evaluated in the light of Australasian Standard SAA/SNZ MP77:1998: A Definition of Year 2000 conformity requirements ('the standard').

9.6.3 Guidelines

(i) Reporting format

The statement required to be published under this Direction should include information on the type in the following example:

Critical Business or System Name	*Plain English Description of Critical Business Function*	*Scheduled Actual Date for Year 2000 Compliance*
System 'x'	Dispensing chemicals into a public water supply	August 1998
System 'y'	Land tax assessment and collection	September 1998
System 'z'	Medical Equipment within <*a particular*> hospital	April 1999

Where a principal reporting entity has a business critical system which is controlled, operated or maintained by another organisation (including another reporting entity), that system should be included in the principal entity's compliance statement. A department is not required to report on compliance in relation to public bodies except to the extent that those public bodies use systems controlled, operated or maintained by the department.

Where a reporting entity relies upon an electronic interface with third party such as a bank, a supplier and/or a client, the system interface should be included in the organisation's compliance statement. The description of the key function(s) of each system should be expressed in non-technical language suitable for a general purpose report to the community.

(ii) Australasian Performance Standard

The Standard to be observed defines conformity as follows:

> 'Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during or after the year 2000. In particular -
> *Rule 1*. No value for a current date will cause any interruption in (the reporting entity's) operation;
> *Rule 2.* Date-based functionality must behave consistently for dates prior to, during and after the 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; and
> *Rule 4.* Year 2000 must be recognised as a leap year in terms of handling both the 29th February and day 366'

The Standard explains certain aspects of the four rules as follows:

Rule 1
If this rule is satisfied, roll-over between all significant time demarcations (eg. days, months, years and centuries) will be performed correctly;
Current date means today's date as known to the equipment or product.

Rule 2
This rule means that all equipment and products must calculate, manipulate and represent dates correctly for the purposes for which they were intended. Functionality includes both processes and results of those processes.

No equipment or product is to use particular date values for meanings; eg. '99' to signify 'no end value' or 'end of file' or '00' to mean 'not applicable' or 'beginning of file'.

Rule 3

Explicit representation of the year in dates may be by using four digits or by including a century indicator. Inferencing rules mean, for example, two-digit years with a value greater than 50 imply 19XX, whereas those with a value equal to or less than 50 imply 20XX. Rules for century inferencing as a whole must apply to all contexts in which the date is used, although different inferencing rules may apply to different date sets.

In order to encourage a uniform approach to date fields, organisations should follow the *Time-Date Data Transfer and Presentation Formats Policy,* issued by the Department of State Development in December 1997.

Appendix 9

Year 2000 Compliant agencies

Public Hospitals

Lorne Community Hospital
Wimmera Health Care Group
Manangatang and District Hospital
Beaufort and Skipton Health Service
Queen Elizabeth Centre
Bethlehem Hospital Incorporated
Maldon Hospital

Municipal Councils

Pyrenees Shire Council

Regional Water Authorities

North East Region Water Authority
Grampians Region Water Authority
East Gippsland Catchment Management Authority

Public Bodies

Infertility Treatment Authority
Legal Practice Board
Nurses Board of Victoria
Harness Racing Board
Geelong Performing Arts Centre Trust
Docklands Authority
Victorian Meat Authority
Trust for Nature (Victoria)
Dental Board of Victoria
Psychologists Board
Energy Efficiency Centre
Plumbing Industry Board
Museums Board of Victoria
Tomato Industry Development Committee
Parliamentary Trustee
Water Training Centre
Victorian Strawberry Industry Development Committee.

Companies, Trusts and Joint Ventures

La Trobe University Union
Tricontinental Corporation Limited
Melbourne Convention and Exhibition Trust
RMIT Foundation
Melbourne Sports & Aquatic Centre Trust
Monash IVF Pty Ltd
Monash IVF Pathology Services Trust
Melbourne Research Enterprises Ltd
Melbourne 2006 Commonwealth Games Bid Pty Ltd
Victorian Institute of Sport Ltd

Regional Library Corporations

Swan Hill Regional Library Corporation
West Gippsland Regional Library Corporation

Public Cemeteries

Cheltenham and Regional Cemeteries Trust
Trustees for the Lilydale Memorial Park and Cemetery
Geelong Cemeteries Trust
Bendigo Cemeteries Trust
Trustees for the Memorial Park Altona
Keilor Cemetery Trust
Anderson's Creek Cemetery Trust

Ballarat General Cemeteries Trust

Regional Waste Management Groups

South Eastern Regional Waste Management Group
Northern Regional Waste Management Group
Eastern Regional Waste Management Group

Appendix 10

COSTS OF THE YEAR 2000 PROBLEM

Company	***Cost Estimate $(million)***
AMP Ltd	135, 500[a]
Telstra	500
Victorian Government	410[b]
NAB	255
ANZ	183, 200[c]
Qantas	147
Commonwealth Government	600[c]
Queensland Government	136[c],200[d], 280[e]
Orica	120
Commonwealth Bank	115
Optus	115
NSW Government	104[c]
Coles Myer	90
BHP	85
SA State Government	78[c]
Lend Lease	75
Westpac	60
Amcor	53
St George	50
TNT	45
Colonial	40
News Ltd	40
Boral	40
Coca-Cola Amatil	30
Woolworths	30, 25[c]
CSR	20
Victorian Electricity companies [f]	1 to 15
Goodman Fielder	10
Pasminco Ltd	7

Notes

(a) All figures based on ASX 1998 company filings except as noted, for example. $500 million based on a report in the press.

(b) Extrapolation of the Committee's Year 2000 survey result ($340 million)

(c) *The Australian Financial Review*, 12 October 1998. Special Report, p.30

(d) Queensland Parliament, Public Accounts Committee, *The Australian Financial Review*, 13 March 1998, p34.

(e) Minister for Information and Communication, Mr Terry Mackenroth, *The Australian*, 28 July 1998, p.38.

(f) Evidence taken at Private Hearings, PAEC, 21 August 1998 and 10 September 1998. Costs for the Distribution network - includes planning and assessment costs only.