1999

PARLIAMENT OF TASMANIA

AUDITOR-GENERAL SPECIAL REPORT NO 30

YEAR 2000: COMING READY OR NOT

No 2 of 1999 – September 1999

Presented to both Houses of Parliament in accordance with the provisions of Section 57 OF THE Financial Management and Audit Act 1990

By Authority:

Government Printer, Tasmania

Auditor-General's reports are available from the Tasmanian Audit Office, HOBART. This report and the recent titles shown at the back of this report can be accessed via the Office's home page. For further information please contact:

Tasmanian Audit Office
GPO Box 851
Hobart
TASMANIA 7001

Phone: (03) 6233 4030, Fax (03) 6233 2957
Enmail: admin@audit.tas.gov.au
Home Page: http://www.audit.tas.gov.au

This report is printed on recycled paper.

ISBN 0 7246 7234 6

21 September 1999

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear Mr President
Dear Mr Speaker

PERFORMANCE AUDIT NO 30
THE YEAR 2000: COMING READY OR NOT

This report has been prepared consequent to examinations conducted under section 44 of the Financial Management and Audit Act 1990, for submission to Parliament under the provisions of section 57 of the Act.

Performance audits seek to provide Parliament with assessments of the effectiveness and efficiency of public sector programs and activities, thereby identifying opportunities for improved performance.

The information provided through this approach will, I am sure, assist Parliament in better evaluating agency performance and enhance Parliamentary decision making to the benefit of all Tasmanians.

Yours sincerely

A J McHugh
AUDITOR-GENERAL

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AFAC	Australasian Fire Authorities Council
BERM	Business Entity Risk Manager
BIOS	Basic Input Output System
BOMA	Building Owners and Management Authority
BPO	Business Process Owners
CACS	Command and Control System
CADIS	Computer Aided Dispatch Information System
CBU	Consulting Business Unit
CEO	Chief Executive Officer
CMT	Corporate Management Team
COSOPS	Critical Operations Standing Operating Procedures
DHHS	Department Health and Human Services
DIER	Department of Infrastructure Energy and Resources
ECC	Energy Control Centre
ECS	Energy Control System
EDACS	Ericsson Digital Radio Network
EFT	Electronic Funds Transfer
EMT	Executive Management Team
ESAA	Electricity Supply Association of Australia
FEP	Front End Processor
FIRECOMM	The command and control centre of the Tasmania Fire Service
FIRM	Fire Incident Response Management System
FTE	Full Time Equivalent
HRIS	Human Resource Information System
HRMIS	Human Resource Management Information System
HTML	Hyper-Text Mark-up Language
IMB	Information Management Branch
IMP	Incident Management Plan
IMT	Issues Management Team
ISDN	Integrated Services Digital Network
ISO	International Standards Organisations
IT	Information Technology
ITSS	Information Technology Services and Solutions

LAN	Local Area Network
LCC	Launceston City Council
LGH	Launceston General Hospital
LGIS	Local Government Information System
MEM	Municipal Emergency Management Plan
MMIS	Materials Management Information System
MW	Mega-Watt
NWRH	North West Regional Hospital
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PDS	Process Data Systems
PLC	Programmable Logical Controller
PMO	Project Management Office
PSTN	Public Switched Telephone Network
QA	Quality Assurance
RDC	Regional Disaster Controller
REMP	Regional Emergency Management Plan
RHH	Royal Hobart Hospital
RFDS	Royal Flying Doctor Service
RTA	Road Traffic Authority
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCATS	Sydney Coordinated Area Traffic System
SES	State Emergency Service
SMUG	SCATS Management Users Group
SOPS	Standard Operating Procedures
TEMP	Tasmanian Emergency Management Plan
TESI	Tasmanian Electricity Supply Industry
THAC	Tattersalls Hobart Aquatic Centre
VAX	Virtual Address extension (minicomputer server)
VCR	Video Cassette Recorder
VMS	Virtual Memory System (operating system)
WWTP	Wastewater Treatment Plants
WY2K	Whole of Government Year 2000 Project
Y2K	Year 2000

INTRODUCTION

Under the provisions of section 44(b) of the *Financial Management and Audit Act 1990* the Auditor-General may

> 'carry out examinations of the economy, efficiency and effectiveness of Government departments, public bodies or parts of Government departments or public bodies.'

The conduct of such audits is often referred to as performance auditing.

This report relates to a performance audit carried out by the Tasmanian Audit Office during the period February to August 1999 of the Year 2000 (Y2K) activity undertaken by essential service providers.

Last year in Special Report No 25 of March 1998 (The Year 2000 - Are We Ready?) findings made as a result of a survey of Y2K readiness of government organisations were published. In that report the following recommendation was made:

> 'A whole of Government approach should be adopted to coordinate the public sector response to the Year 2000 Problem, with the establishment of a steering committee at the most senior levels of the public sector.'

Consequently, the Government appointed a Senior Project Manager in the Whole of Government Project Unit within the Department of Premier and Cabinet whose function it was to coordinate the Tasmanian Government Y2K-related activities. The Senior Project Manager has supervised the collection and public dissemination of statistical information about the readiness of government agencies to deal with the problem. The Government is to be commended for disclosing this information to the public on a monthly basis.

Early in 1999 the Auditor-General took advice as to whether a follow-up audit should be conducted. The audit was authorised with the scope limited to entities supplying 'essential services', e.g. water, electricity, police, etc.

Most of the field work was carried out in March 1999 – June 1999. Very detailed written reports were prepared and supplied to the auditees. These reports included an Audit Office semi-quantitative assessment of Y2K readiness at that time. Since then there have been several monthly reports made public by the Whole-of-Government Year 2000 Project (WY2K) team and steady progress has been made.

There was therefore little point in providing statistics in this report on the situation as it existed at the time of the audit. The current position is better ascertained from the Whole-of-Government report. In addition, some entities have elected to provide a brief summary of progress they have made since the field work was conducted and that information has been included by way of comment in this report.

This audit has therefore already made two valuable contributions to this topic. First, each entity audited had an independent assessment of its approach to Y2K activity. Second, the Whole-of-Government Project Unit gained additional assurance that the information provided to it and thence to the public was soundly based.

The monthly statistics provided to the public are of necessity highly summarised and deal with entities across the whole of the public sector. With the release of this report, Parliament and the public can obtain a more detailed picture of the efforts that have been made to address the potential problem focussed on those areas that are critical to the well-being of the Tasmanian community.

AUDIT OPINION

Report Title	The Year 2000 – Coming Ready or Not
Nature of the Audit	The objective of this performance audit was to report on the progress made by essential service providers in relation to testing, compliance business continuity and governance for those systems and processes defined as critical by Government Agencies.
Responsible Parties	Executive Government, Heads of the relevant Agencies, and Chief Executive Officers of relevant public sector entities.
Mandate	This audit has been carried out under the provisions of Section 44(b) of the *Financial Management and Audit Act 1990* which provides that: *'The Auditor-General may carry out examinations of the economy, efficiency and effectiveness of Government departments, public bodies or parts of Government department or public bodies.'*
Applicable Standards	This audit has been performed in accordance with Australian Auditing Standard AUS 806 "Performance Auditing".
Limitation on Audit Assurance	Audit procedures were restricted to a review of documentary evidence and discussions with relevant officers of each entity. Some of the documentary evidence could not be provided at the time of the audit. The evidence provided by these procedures restricts the audit assurance to a moderate level, as the evidence is persuasive rather than conclusive in nature.
Audit Criteria	The status of the critical systems and processes was assessed against the following criteria: *Testing* • *Has checking with suppliers taken place in respect of the status of systems or equipment?* • *Has physical testing of systems been undertaken?* *Compliance* • *Have compliance criteria been defined?* • *Have remediation and end-to-end testing been conducted?* *Business Continuity* • *Has a risk assessment bee done?* • *Have contingency plans been developed?* *Governance* • *Has the project been adequately supported by senior management?* • *Have reporting channels project schedules been followed?*

Opinion and Conclusions

I have noted during the audit that:

- Substantial progress has been made by the majority of public sector entities in the testing of systems and processes identified as being critical;
- Remediation of non-compliant systems was in progress but not substantially complete at the time of the audit;
- A number of entities planned to conduct end-to-end testing after remediation had been completed;
- Risk assessment had been completed by the majority of entities;
- Contingency planning was in a preliminary stage of development for the majority of entities;
- All entities had disaster plans that to various extents addressed possible emergency scenarios arising from the Y2K problem;
- Project sponsors had been nominated and steering committees or task forces convened in all cases;
- Access to and allocation of resources for projects was satisfactory for most entities;
- All entities were participating in the Whole of Government Public Disclosure reporting process; and
- A number of entities made use of the project management tools to assist with planning and scheduling of projects.

All entities demonstrated commitment to the minimisation of exposure to the Y2K problem. This was confirmed through the implementation of methodologies that were geared to ensuring the compliance of technology and business continuity. Considerable resources had been dedicated to testing and remediation of critical systems and processes; provided efforts are sustained at this level, the probability of incidents arising due to technological failure should be minimal. For the most part Y2K-specific contingency planning was in a preliminary stage of development at the time of the audit.

I conclude that owing to the sizeable amount of effort that was still to be expended at the time of the audit to the development and refinement of contingency and emergency plans, the Audit Office cannot provide assurance that business operations will continue unimpeded. Resolve demonstrated by project managers to meet milestones and priorities accordingly is, however, an indication of the high level of commitment to finalise the task successfully.

RESPONSE FROM THE DEPARTMENT OF PREMIER AND CABINET

The response from the Acting Secretary was dated 8 September 1999 and her comments follow:

> 'Thank you for your opportunity to view the draft Report to Parliament in relation to the Performance Audit – Year 2000 Follow-up.
>
> As you are aware, the Whole of Government Y2K Project Steering Committee had raised concerns in relation to levels of Y2K readiness and preparedness in the provision of essential services to the community at both State and Local Government levels. The information contained in the Report is comprehensive and will be of assistance to the organisations concerned.'

AUDIT OBJECTIVES, SCOPE, CRITERIA, TIMING AND COST

AUDIT OBJECTIVES

The primary objective of the audit was to gauge the Y2K preparedness of auditees. This involved preparation of this Report which:

- Summarises project effectiveness in line with audit criteria; and
- Reviews the progress made by auditees.

The secondary objective was to provide feedback to auditees on the effectiveness of Y2K projects during the course of the audit. This involved writing more detailed reports which:

- Identified limitations and made recommendations where appropriate; and
- Recognised effective use of methodologies or tools and noted these as examples of best practice.

SCOPE OF THE AUDIT

The review covered the following providers of essential services to the community,

- Hobart City Council;
- Launceston City Council;
- Royal Hobart Hospital;
- State Emergency Service;
- Tasmania Ambulance Service;
- Tasmania Fire Service;
- Tasmania Police;
- Tasmanian Electricity Supply Industries; and
- Traffic Management Branch (Department of Infrastructure Energy and Resources).

AUDIT CRITERIA

Criteria examined by the Audit Office in relation to Y2K activities were:

Testing	physical testing and status checking with suppliers;
Compliance	remediation of non-compliant systems;
Business Continuity	actions to ensure unimpeded business operation; and
Governance & Reporting	Internal management structures and information flow.

AUDIT TIMING AND COST

Planning for the performance audit commenced in February, testing occurred in March through to July 1999 and the report was finalised in August 1999.

The total cost of the audit, including the cost of Tasmanian Audit Office staff but excluding report production costs is estimated at $119 000.

AUDIT METHODOLOGY

At its meeting on 3 April 1998, the Budget Committee endorsed a quarterly monitoring and reporting process in relation to the Y2K Problem which was to be coordinated by the Department of Treasury and Finance and the Department of Premier and Cabinet. For the purposes of consistency in reporting within the Budget Committee framework critical systems and processes were subsequently defined as having:

> '...the potential to cause disruption to the continuity of the delivery of 'key' services by each entity (ie those services identified for public disclosure purposes) **OR** those whose continuity have the potential to jeopardise the health, well-being and safety of people in Tasmania.'

In devising a suitable methodology the Audit Office focussed on critical systems and processes identified by auditees consistent with this definition (ie non-critical systems and processes were not subject to audit). The methodology employed a top-down analysis of the key areas of the Budget Committee survey. The audit criteria were testing, compliance, business continuity and governance. In each of these areas the questions used by the Audit Office to determine progress and coverage were also derived from the budget survey. Detailed questions based around the core criteria were developed from a variety of sources to allow in-depth analysis. A steering committee with representatives drawn from project teams of various governmental agencies provided input to development of the audit methodology. The components examined are listed below:

Testing	• Information Technology (IT) • Building and Environment • Telecommunications • Other Embedded Technology • In-going / Out-going Supply Chain
Compliance	• IT • Building and Environment • Telecommunications • Other Embedded Technology • In-going / Out-going Supply Chain
Business Continuity	• Risk Assessment • Contingency Planning • Contingency Criteria • Staff Training – Contingency Planning • Contingency Testing
Governance	• Project Sponsor • Reporting • Timelines • Research/Information Gathering • Awareness Raising

The Budget Committee also sought information in respect of risk/confidence ratings for the following components, which were also reported to auditees.

Risk / Confidence

- Public Safety and Welfare
- Service Provision
- Revenue Generation and Payment
- Legal Liability
- Security and Confidentiality

Auditees provided ratings in respect of likelihood and impact of risk for these categories. A semi-quantitative method, consistent with Australian Public Service guidelines for managing risk, was used by the Audit Office to rank the ratings. This exercise was performed fundamentally as a check of the risk ratings submitted and, because the results were highly generalised as well as being dated, they have not been included in this report.

BACKGROUND

CHRONOLOGY

The Y2K Problem is widely acknowledged as a potential threat to the continued operation of government entities. Special Report No 25 of March 1998 (*The Year 2000 - Are We Ready?*) described in general terms the nature of the problem and the possible effect on government services and operations.

As a response to recommendations in the report, the Department of Premier and Cabinet noted that the difficulty in establishing an assessment of business-focussed risk management arose from an historical technology focus. This had involved development of a comprehensive inventory and the testing of each item for compliance against Y2K standards. It was therefore proposed that the State adopt a methodology which sought to establish business continuity planning as the Y2K strategy.

A model which made provision for the development of alternative arrangements to ensure business continuity in the event of technology failure was devised. This model provided for the preparation of contingency plans as well as for the testing and remediation of technology thereby ensuring thoroughness through both a top-down and bottom-up approach.

In order to expedite the process across the public sector it was recommended that some form of whole of government facilitation and support be provided. Consequently, the Budget Committee endorsed the coordination of a quarterly monitoring reporting process by the Department of Treasury and Finance and the Department of Premier and Cabinet. The reporting framework was designed to assess agencies' progress against the business continuity planning methodology and reinforce the approach of addressing the problem as a major risk to core business. Three sets of reports were submitted to the Budget Committee in total – these were provided in May and October 1998 and February 1999.

Senior management workshops were then held to provide an overview of the business continuity methodology and give agencies some direction and initial impetus to implement this approach. Deliverables from the workshops included the documentation of outlines of key business activities and contingency plans prioritised according to outcomes to the community, and agreement on a high level work plan identifying leadership roles and business manager responsibilities.

Following the change of Government in September 1998 the Whole of Government Year 2000 Project (WY2K) was launched. Currently the Project Team consists of 6.5 Full Time Equivalent (FTE) positions and provision has been made for additional skills and resources to be acquired as needed.

Outputs of the project defined in the WY2K Business Plan included the provision of:

- Agreed and documented Y2K contingency planning for the Tasmanian public sector;
- Audits of critical services provided by Government agencies to business and the community, to confirm agency preparations;
- Facilitated liaison between the State Government and other governments, major service providers, community groups and industry bodies;
- Regular reports and analyses (in conjunction with the Auditor-General) of the status of preparedness of government entities;

- A Communications Strategy Plan (in conjunction with the Whole of Government Media Office);
- A Tasmanian Contingency Plan (in conjunction with the Department of Police and Public Safety).

In March 1999 all jurisdictions at a State Minister's conference agreed to the public disclosure of information on Y2K readiness. A minimum standard was established that meant each government would disclose on the basis of individual agency readiness. Tasmania chose to disclose similarly but at the service level. The percentage of the work that had been completed in order to make the service ready for the Y2K was to be reported, as was the readiness date and the progress with respect to the project schedule. Shortly thereafter Cabinet made a decision to no longer receive Budget Committee surveys because information provided was not as current as that submitted with the Public Reporting process.

PREVIOUS REVIEWS AND AUDITS

The potential for Y2K Problems to disrupt state and federal organisations has triggered considerable audit activity. A number of reports from other offices were examined as part of the planning for the Tasmanian audit.

Report No 27, *Managing the Year 2000 Problem: Risk Assessment and Management in Commonwealth Agencies* was issued by the Australian National Audit Office in 1997. It was based on a survey questionnaire that agencies completed earlier that year. Later, in 1998 – 1999 Report No 22, *Getting Over the Line: Selected Commonwealth Bodies' Management of the Year 2000 Problem,* progress in 8 Commonwealth bodies that provide key government functions was reported.

The New South Wales Auditor-General issued a report *1999-2000 Millennium Date Rollover: Preparedness of the NSW Public Sector* in 1997. Subsequently, the *New South Wales Auditor-General's Report to Parliament for 1998* gave an account of a special review conducted on the impact of Y2K on critical services based on a self-assessment survey questionnaire that had been circulated to a range of service providers in mid 1998.

In 1999 the Auditor-General of the Australian Capital Territory issued Report No 2 *The Management of Year 2000 Risks*. This report was produced as a result of fieldwork carried out by performance auditors and contractors in a variety of public sector agencies in the latter half of 1998.

The Northern Territory Auditor-General's Office issued its *End of Financial Year Report to the Legislative Assembly* in 1997 with general observations on Y2K issues made as a result of a performance management system audit. A similar report issued in February 1998 contains updated details as well as specific observations made in respect of Northern Territory essential services. A six monthly update was published in August 1999.

Matters associated with the Y2K Problem were addressed in the Western Australia Auditor-General's Report No 7 *Report on Controls, Compliance and Accountability Audits.* More recently, Report No 1 *Report on the Western Australian Public Health Sector* published in 1999 detailed progress in regard to Y2K Problems in the public health sector.

The Auditor-General of Queensland reviewed Y2K preparedness as an emerging issue in Report No 4 *1998 – 99 Audits on Local Governments*.

At the request of the Auditor-General of Victoria, the Public Accounts and Estimates Committee resolved to undertake an inquiry into the Y2K Problem and the level of preparedness of the Victorian public sector. As a result Report No 26 *Information*

Technology and the Year 2000 Problem – Is the Victorian Public Sector Ready? was produced.

A report issued by the Canadian Office of the Auditor-General in 1997 (*Report of the Auditor-General.* 'Information Technology: Preparedness for Year 2000') also addressed the problem.

AUDIT FINDINGS

TASMANIAN AMBULANCE SERVICE

The information in this section is based on audit activity during April 1999.

Testing

The Service has focussed more on channelling limited resources towards the remediation of known non-compliant systems with contractors, rather than on documentation of a formal approach.

IT Systems

A significant critical IT system for Ambulance Service is the Computer Aided Dispatch Information System (CADIS). This system is responsible for centralised communication, as well as case logging, monitoring and scheduling of vehicle status. It had been found to be non-compliant and was to be replaced with a state-of-the-art solution.

According to the Specification of Requirements for CADIS the contractor had agreed to meet all Y2K conformance standards as required by the Ambulance Service. Acceptance testing procedures determined by the steering committee for the contract were also to be conducted. The non-compliant operating system upon which CADIS resides had been recently upgraded, but the complete installation of the system was not to be completed until 30 June 1999. Documentary evidence of these testing and remediation processes could not be made available to the Audit Office at the time of the audit. The auditee explained, however, that the implementation of the replacement system was well advanced in April 1999.

The industrial control package for the radio network known as Wizcon is another significant non-compliant critical IT system. The failure mode of the non-compliance of this system is such that manual switching would need to be adopted. This would place a major strain on communication personnel and it is likely that the effective operation of the radio network would be compromised. The non-compliance of this system was yet to be addressed by a communications consultant.

Building and Environmental Systems

Authorities providing services such as electricity, water, sewerage and traffic were to be queried in writing to ascertain their status with respect to the Y2K Problem. Water supply is particularly critical to the Service and therefore the status of regional suppliers was to be determined in the near future.

Compliant back-up generators were in place for the Northern and Southern regions, but there was not a generator in the North West region and this was of concern, since failure of supply to this station would render radio communication and computer-aided dispatch impossible. Discussions were being held to determine a solution to this problem.

Telecommunications Systems

The radio control system is a significant non-compliant critical telecommunication system. Capital Improvement Program funding to the value of $20 000 had been committed to the production of a report on the Y2K status of components of this system. The total system test was scheduled for completion by 30 April 1999.

Test specifications were not available at the time of audit, however a checklist did detail equipment to be tested. Items listed included mobile and portable phones, base stations, links (VHF and UHF), inter-region links, state-wide control equipment, Wizcon control software and other dispatch communications services such as TASINET (in-going 000 and non-emergency calls and out-going calls) and radio paging services. Radio paging services are provided by Telstra, Tasmania Fire Service and Ambulance Service overlay pagers; the Ambulance Service was yet to seek compliance statements from each of these providers.

The Ambulance Service obtained a letter from Networking Tasmania stating that it would be able to advise on compliance of voice and data networks only when Telstra released their standard compliance statement to the Government in May 1999. Some voice loggers utilised by the service were non compliant and while the vendor had been requested to replace these, this had not been done at the time of the audit. A caller line identification capability was intended to be built into CADIS and it was expected that this would be compliant.

Helicopter Resources and the Royal Flying Doctor Service (RFDS) use global positioning systems and information on their Y2K status had been requested. The response from Helicopter Resources stated that it was currently seeking information from relevant aircraft equipment manufacturers and that it expected to be able to provide information on its Y2K status by June 1999. The RFDS stated that systems used by this service were compliant.

Other Embedded Systems

Biomedical testing notes and a database listing compliance of biomedical equipment had been obtained from the New South Wales Government Y2K web site. Critical biomedical systems had been listed for checking and these included defibrillators, pulse oxymeters and blood pressure equipment, syringe pumps, oxygen equipment and glucometers.

Compliance details for most equipment could be obtained from the biomedical database; however, some items of equipment could have contained different embedded chips than those in the equipment tested by manufacturers. As a precaution the Service planned to conduct tests on biomedical equipment where variation in the chip types used was suspected. Testing was to continue until June 30 1999 on biomedical devices that were suspected to be non-compliant.

A letter had been sent to the major supplier of ambulance vehicles requesting information on the Y2K status of vehicle systems and equipment and the Service was still awaiting a reply at the time of audit. Uninterruptable power supplies had been checked and found to be compliant.

In-going and Out-going Supply Chain

This area was planned to be addressed fully when the Good Samaritan Legislation was confirmed. The Y2K status of providers of day-to-day medical consumables was also to be determined.

Compliance

A formal compliance plan had not been developed at the time of the audit. A comprehensive framework had been obtained from the Queensland Ambulance Service however, and this was to be completed in due course. The Australian Standards of compliance were to be adopted as compliance criteria for all devices and systems.

Business Continuity

A Project Plan for the Department of Health and Human Services (DHHS) detailed the objectives and scope of the Y2K project for the agency. These included full documentation of all aspects of Y2K work through to the categorisation of key business activities and the development of contingency plans.

A specific project plan of this type had not been developed for the Ambulance Service and as a result a coordinated approach was lacking.

Risk Assessment

A draft assessment in the form of a business risk analysis had been partially completed and critical systems had been identified although they had not been formally documented. The format of the assessment was qualitative and based on New Zealand Standards. It used a assessment matrix to categorise risks and recommendations for action were based upon risk categories.

Contingency Planning

A contingency framework titled Critical Operations Standing Operating Procedures (COSOPS) had been obtained from the New South Wales Hospital Service. The Ambulance Service was to begin filling in this framework at the time of the audit and the intention was to have it completed by 30 April 1999.

The Service also had Emergency Management Plans which would form part of the overall Y2K contingency plan and to this end, contingency planning could be considered to be partially completed.

Other proposed contingencies include the use of vehicles as base stations and the use of aircraft as back-up radio links in the event of a remote repeater site failure. These and other contingencies still needed to be fully documented.

Criteria for Contingency Mode

The COSOPS framework had provisions for addressing staff roles and responsibilities with respect to the contingency plan. The Service intended to complete this aspect of contingency planning by 30 September 1999 and this was considered to be an achievable target date.

Staff Training

The COSOPS framework had provisions for addressing staff roles and responsibilities with respect to the contingency plan and this task was also to be completed by 30 September 1999.

Contingency Testing

The Service intended to complete testing of contingency plans by 30 September 1999.

Governance

Significant shortcomings in the area of governance and reporting appeared to have occurred in the past in relation to the resourcing and reporting of the project. In particular, lack of funds had been cited as a contributing factor for slow progress in all aspects of the project.

Project Sponsor

The project had a sponsor since its inception in 1997. However, in the earlier stages it was not given the priority required for adequate progress and this resulted in a large number of tasks being left until 1999. According to the auditee, however, the current sponsor since taking on the role in December 1998, has made this project one of the top priorities of the Agency.

The Project Manager was advised by the Senior Business Advisor that the Funding Review Committee had concluded there was no capacity to provide additional funding for the Y2K project as a new initiative. Accordingly Y2K costs were to be funded by Divisions. A project expenditure estimate for 1998-1999 was not provided to the project manager by the Hospitals and Ambulance Service, however for 1999-2000 the expenditure estimate provided for the Ambulance Service was $84 000.

The coordinator for the Ambulance Y2K project indicated that he had not been allocated any time release from his normal course of duties for the project and he suggested that one additional FTE on the project in Ambulance was required.

Reporting

The Y2K steering committee provides written reports on a monthly basis to the project sponsor on the progress of DHHS as a whole. The Business Risk Manager for the Hospitals and Ambulance Service is a member of this committee and he has reported verbally there on the progress of the Ambulance Service. Written reports on the progress of the Ambulance Service however, have not been provided. There were no references to the progress of the Ambulance Service in either the February or the March minutes of steering committee meetings.

The Ambulance Public Disclosure readiness percentage of 59% for March 1999 implied that over half of the effort required to attain readiness had been applied. As documentary evidence of testing and remediation of several critical systems was not able to be supplied at the time of the audit, it was difficult to ascertain the accuracy of this figure. The overall percentage representation for Contingency Planning given was 30%, and this was broadly in agreement with audit findings.

An October 1998 survey response indicated that contingency plans for critical systems and processes had been completed, however, the response for the same question on the February 1999 survey indicated that the development of contingency plans was in progress and drafts would be completed by 30 April 1999. The February response was in agreement with the audit findings. Also, responses to the questions on testing for the October 1998 survey indicated that the agency had developed a comprehensive testing plan which addressed all systems. The February 1999 survey however, contradicted the earlier response by indicating that a comprehensive testing plan had not been developed and it was not in progress. Another response given in the same survey was also not in agreement with audit findings, as no formal test plans for any systems had been developed.

Comment from auditee:

'DHHS has contended that the discrepancies in responses to the Budget Committee surveys to a large extent reflect the poor survey design, which had insufficient instructions attached to ensure correct interpretation of the meaning of various questions, [and that as a result] *... the impression created was that the Agency was further advanced with the detail of its Y2K planning than in fact it was.'*

Timelines

The timeline for completion documentation of the risk assessment was April 1999 and this was considered to be relatively late in the process. Also a formal project schedule had not been compiled at the time of the audit.

Information Gathering

The Ambulance Service had gathered information from a range of sources including the Internet and peers.

Awareness-Raising Activities

The project manager had published two newsletters and the Intranet was used to share Y2K information across the DHHS network. Several educational workshops had been conducted on the progress of the project.

Conclusion

The Service had prioritised and devised measures of remediation for critical systems, however, the formalisation of this process through concise documentation was still to be undertaken.

Auditee Update

'Following the Audit undertaken in April 1999, significant progress has been made. Milestones achieved include:

- *The non-compliant CADIS was successfully replaced with CAD2000+ in May at a cost of $320 000.*
- *A back-up generator has been supplied to North West Ambulance at Burnie*
- *A full test of the radio control system was completed in May. While the Wizcon radio switching unit is strictly non-compliant, testing reveals that its failure mode is such that continuity of communications will not be affected. A new voice logging system is scheduled to be installed by 25 August. The Government has recently allocated $305 000 to the upgrade of the Ambulance communications system.*
- *Helicopter Resources and the Royal Flying Doctor Service have advised that their systems are compliant.*
- *Testing of critical biomedical equipment has been completed and all items are Year 2000 Compliant.*
- *The Y2K status of vehicle systems and equipment for ambulance vehicles has been confirmed as Year 2000 Compliant.*
- *A comprehensive risk register has been developed which documents the initial risk assessment, the expected result following remediation and mitigation strategies and progress to date. This is updated monthly to monitor the progress of risk reduction.*
- *Contingency plans that support the existing Emergency Management Plans have been developed and staff training and testing is in progress. This will be largely completed by 30 September, although on-going refinement will continue in the last three months of the year.*

The Tasmanian Ambulance Service is confident of the validity of the readiness reporting it is providing for public disclosure. At the end of July 1999, overall readiness for the Ambulance Service was 91%. This comprises:

Component	***Readiness***	***Weighting***
Road and Air Transport	*99%*	*20%*
Biomedical Equipment	*99%*	*25%*
Support Systems	*97%*	*25%*
Contingency Planning	*74%*	*30%*

The public can be confident that the Tasmanian Ambulance Service will be fully prepared for the year 2000.'

TASMANIA POLICE

The Audit Office carried out a review of Tasmania Police during April 1999.

Testing

Tasmania Police had developed comprehensive formal testing plans for IT and telecommunication systems. For building and environmental systems a test plan had not been prepared, however, a detailed spreadsheet that summarised the progress towards compliance for all buildings was regularly updated. Also, action plans had been developed by a consulting firm for testing of police building systems and a comprehensive testing framework was obtained from the Building Owners and Management Authority (BOMA) web site. Material required for the development of a testing plan for building and environmental systems was therefore available and minimal effort was required to document the approach in a formal plan. For other embedded systems, a plan had also not been developed and investigation of the value of such a document was still to be conducted. It was not considered necessary to develop a formal plan for the management of in-going and out-going supply chain as most processes and systems that could be classified in this category had been addressed by other plans.

IT Systems

A comprehensive test plan had been developed for critical IT systems based upon the Standards Australia definition of compliance. Within the Service the use of IT was extensive and decisions to undertake remediation were based upon a well-documented risk assessment. In order to be classified in the highest or critical level of risk a component had to comply with the following definition:

> 'an operational system, the short term failure of which or the provision of incorrect information may lead to death, injury or serious loss of property.'

Systems in this critical category were the Command and Control System (CACS) (client and host) – an application which manages and monitors the dispatch of resources; the Firearms Client – a database register of licensed firearm holders; Solaris – the Unix based operating system and TPSS – the Security Logon System and UniVerse command languages.

For the most part, critical applications had been developed in-house so that testing and remediation involved scanning of source codes for all date formats and the subsequent conversion of year formats from two-digit to four digits. According to the project management schedule, the testing of CACS was originally due to be completed by 30 April 1999. This was later revised to 30 June 1999 because of hardware problems and staff shortages in IT support.

A summary progress report revealed that all Personal Computer (PC) based Firearms programs were compliant, but there was still a need to test the host and NT-based component of the system.

The Sun Microsystem's web site indicated the need for modifications to be made to the versions of Solaris used by the Service. According to the project management schedule, it was anticipated that the prescribed fixes would be applied by 30 May 1999.

Although it was not expected that the TPSS Security Logon System had any date dependency, testing and system remediation was scheduled to be completed by 30 April 1999. Syntax checks of dates used by the command language were undertaken and according to the project schedule, full compliance was expected by 30 May 1999.

Full end-to-end testing of all critical IT systems was to be completed by 30 September 1999, once compliance of individual systems had been attained. Given that the Service provided evidence of a high level of in-house expertise through comprehensive documentation of appropriate testing processes, it could be expected that compliance would be achieved for critical systems within the prescribed timelines.

Salary payment through the human resource package REMUS had been identified as a critical system for Tasmania Police and while the current version of this package was not compliant, a contractual arrangement with the REMUS consortium for an upgrade was expected to guarantee compliance. Documentary evidence of the intended upgrade, however, was not available at the time of the audit.

Building and Environmental Systems

The buildings which house critical systems for Tasmania Police are Operations Support and the Southern, Northern, Western and Eastern district command stations.

Systems at the Operations Support building had undergone extensive testing with live tests in October of 1998. Testing of the City Police building had been inconclusive, as the generator supplied no power at all to this complex. According to the Buildings Status Report the security systems and the Direct Digital Control system (that controlled the internal environment) were being replaced and remediation was partially completed for other systems. Also, changes had been made to the wiring from the generator set to the City Police building, but these changes were yet to be tested.

The status of the Launceston District Command station was of most concern because emergency power was only available to the small part of the building that housed communications. Additional funding of the order of $20 000 to $30 000 was required for the wiring upgrade. The building systems were to undergo end-to-end testing along with all other systems by 30 September 1999.

Telecommunications Systems

The Communications Services Branch test plan had identified six critical systems. These were the fixed phone network, customer premises equipment, the mobile phone network, the radio control system (Centracom), the Ericsson Digital Radio Network (EDACS), the conventional radio system and power supply.

For most of the non-compliant components of the fixed phone network, advice was being sought from Telstra as to the remediation measures to be undertaken. Critical customer premises equipment, including the police academy Private Automatic Branch Exchange (PABX) and Integrated Services Digital Network (ISDN) phones were to be replaced. Also advice was being sought from the suppliers, as to appropriate remediation measures, for the non-compliant terminal adaptors and multiplexers. All phones and components of the mobile phone network apart from Telstra's satellite communications phone had been found to be compliant. No comment as to remediation measures for this phone had been given.

In respect of Centracom, the Service was waiting on software and encoder upgrades from the manufacturer. The service was also awaiting an upgrade from the manufacturer for particular components of the EDACS system. The conventional radio system had been tested and all components found to be compliant with the exception of radio services software for which an upgrade had been ordered.

All uninterruptable power supplies had been tested and, apart from one, they were found to be compliant. Also, power supply to the Service was to be fully tested by the Tasmanian Electricity Supply Industries.

It should be noted that for a number of the components cited above, contingency plans already existed to ensure the continued operation of systems. For example, in the event of failure of the digital radio network the conventional analogue network could be used. Further, in the event of failure of the supply of electricity back-up generators could provide an alternative supply.

Other Embedded Systems

Critical embedded technology included breathalysers and vehicle ignition systems. For breathalysers, an e-mail had been sent to the Traffic Management Branch of the Department of Infrastructure Energy and Resources (DIER) (the provider of breathalysers) to determine their status, however, at the time of the audit compliance had not been confirmed. Also the Fleetcare web site had been examined to determine the status of police vehicles, although documentary evidence in support of this had not been obtained.

In-going and Out-going Supply Chain

Stakeholders including suppliers had been listed in each of the IT and telecommunications plans and reports. As described above testing of a number of key areas had been done by compliance checking with suppliers.

Compliance

Testing plans addressed the requirements for compliance, namely acceptance testing, end-to-end testing and certification of results. When remediation was completed date fields for all applications were to use a four-digit format to represent the year, ensuring that date-based functionality should be achieved for all exception dates. Documents supplied to the Audit Office indicated that full remediation of critical systems should be achieved as a result of end-to-end testing for each of the system areas listed above by 30 September 1999.

Business Continuity

A comprehensive IT Y2K Continuity Project Plan had been developed which covered the project objectives and scope, project management, stakeholder management, financial management, risk management, development schedules and quality management. The plan identified three areas where quality assurance was required: documentation, test accuracy and correctness of fixes. Documentary evidence indicated that quality management had been applied in each of these areas.

Risk Assessment

Risk categories had been defined for the project plan and were applied in the development of testing and remediation programs. The use of clear definitions had enabled branches to prioritise tasks accordingly.

Contingency Planning

Business continuity for Tasmania Police was based upon the activation of the organisational structure and processes described in the Major Incident Standing Operating Procedures. Operation Orders were constantly practised and used in real events (eg warship visits). Within any year, Tasmania Police was likely to have written and implemented over 110 such orders and for this reason contingency planning for Y2K could be considered to be partially complete.

Milestones for the adaptation of these plans for Y2K had been briefly summarised in a draft contingency plan. It appeared that the majority of the minimisation strategies had been conceptualised and noted. Details of these strategies were, however, still to be fully determined and documented.

Tasmania Police intended to operate in a semi-contingency mode of minimised risk before, during and after 31 December 1999. This could involve, the use of back-up generators for the supply of power, the de-linking of critical systems such as CACs from non-critical systems to minimise the exchange of inaccurate date-related data and the switching off of non-critical building systems such as lifts. Such an approach would assist the Service to be more confident in their ability to provide continuity of business in the event of a range of system failures.

Criteria for Contingency Mode

A sample Operation Order examined indicated that criteria for invoking, revoking and functioning in a changed mode of operation were documented. The service intended to develop Y2K criteria for the full contingency plan and given that a breakdown of milestones had been documented, it would be reasonable to expect that the final milestone of 30 September 1999 for the completion of all contingency planning would be achieved.

Staff Training

The Operation Order examined indicated that the roles and responsibilities of staff when functioning in a changed mode of operation were defined and documented. In addition, staff familiarity with procedures was considered to be high because of the high frequency with which these orders were implemented. As a further contingency measure, leave had been revoked for all police officers from 28 December 1999 to 14 January 2000.

Contingency Testing

The high frequency with which operation orders were implemented meant that they were regularly tested and reviewed.

Governance

Governance and reporting for the project appeared to be adequate. All staff interviewed were comfortable with the direction and organisation of the project, as well as being confident that milestones would be achieved.

Project Sponsor

The project sponsor is the Deputy Commissioner who had allocated 4.5 FTE positions to the project. Expenditure on the Y2K Problem to date was estimated at $715 000 and it was anticipated that the budget for 1999-2000 would amount to $255 000.

Reporting

The Audit Office was of the opinion that the public disclosure statistics provided by Tasmania Police were at variance with audit findings because the figures nominated by Police were highly conservative. The published percentages were derived from a detailed project schedule which demonstrated thoroughness in all areas and since the figure representing 'effort required' used to determine the readiness percentages was large, the final fraction of effort expended divided by effort required was conservative.

In relation to the readiness and planning target dates of September 1999, the Audit Office was confident that these timelines could be met because documentary evidence, in the form of project schedules, indicated that the allocation of resources and time to specific tasks had been duly considered.

The service had been reporting to the Information Management Board (chaired by the project sponsor) on a two-monthly basis, however, as activity increased the frequency of this written reporting was to become fortnightly. Written reports to the Corporate Management Group (the senior agency executive group) had been provided on a six-monthly basis. These reports were thorough, clear and concise in their documentation of issues of concern. Branch managers also submitted status and problem incident reports regularly to the Y2K project manager and these reports were of a similar quality.

Timelines

Risk assessments were completed and documented before 1 January 1999. The timeline for completion of end-to-end testing was 30 September 1999 and this was considered to be an achievable goal because of the systematic approach that had been adopted.

Information Gathering

Information had been gathered from a range of sources including the Internet (Meta and Gartner groups) and peers (National Information Technology Manager's Forum, Electronic Service's Group, Workshops). Quality assurance had been sought internally in as much as the project manager had reviewed and coordinated the processes implemented by branch managers.

Awareness-Raising Activities

Regular weekly meetings were conducted with staff involved in the project and meetings were to be held with end users of affected equipment at a later date. Other awareness-raising activities included presentations by the project manager to the Electronic Services Group Forums and to the National Information Technology Manager's Forum.

Conclusion

The Y2K project undertaken by Tasmania Police appeared to have been effectively managed and implemented. Providing that the remaining remediation and development of Y2K contingencies proceeds according to schedule the Service should be well placed to manage incidents that may arise.

TASMANIA FIRE SERVICE

The Audit Office carried out a review of the Tasmania Fire Service during April 1999.

Testing

The terms critical, high, medium and low have been assigned to a system according to the extent to which failure of the system would impact upon the ability of the Service to meet the requirements of the mission statement. This states that:

> 'The role of the Tasmania Fire Service is to protect life, property and the environment from the impact of fire and other emergencies.'

The project manager informed the Audit Office that failure of a critical system would prevent the Service from fulfilling the requirements of this mission statement, whereas failure of a system falling into the risk category labelled 'high' would make fulfilling this requirement difficult.

These definitions were not explicitly written into a plan, but rather were implicitly assumed by all branch managers in implementing the project. In order to minimise any confusion in the use of these terms the Audit Office considered that it would be preferable for the Fire Service to document the definitions of these risk categories.

The project team had developed a compliance program which, at the time of the audit, was only partially completed. A decision was made to not complete the program because a project database which was developed at a later stage was considered to be a more suitable working document. Within the framework, however, business processes had been assigned either a high, medium or low value of risk and a table prepared for the completion of project component details.

Preliminary compliance checking of critical systems through contact with vendors and examination of their web sites had been completed at the time of the audit. This information had been collated in a comprehensive Y2K database of all systems (critical and non-critical). Field components of the database included priority (of the system within the project), compliance status, action to be taken, supplier details and contact and reply dates.

A formal plan had been developed to address in-house testing of remediated IT systems, but similar plans had not been produced for testing of critical building, telecommunications, embedded and supply chain systems. The development of an overarching test plan highlighting test standards deemed to be applicable for the Service could act as a useful guide for the development of test plans for each of these areas.

The Service had not devised a project schedule for testing and subsequent remediation and, although the project appeared to be on track, the development of such a schedule would provide assurance that time lines could be met with available resources.

IT Systems

An IT test plan had been developed by the Information Systems Manager which facilitated the collection of information on system details, exception dates, external system interfaces, date field types, compliance testing and certification levels. This plan had been utilised for in-house testing of most critical and non-critical systems. Where suppliers provided acceptance testing guidelines these had been followed instead of the IT testing plan.

An IT testing schedule that defined timelines for the completion of tasks had not been developed. Such a schedule would assist the service to optimise the allocation of resources to ensure that the testing timeline of 30 July 1999 could be met.

The Fire Incident Response Management System (FIRM) had been identified as a critical system within the command and control centre of the Service known as FireComm. The dispatch system FIRM, is responsible for centralised communication and the dispatch of resources. Due to the pivotal functions performed by this system it was categorised as having critical strategic value with a potential critical impact on the delivery of service if it failed to function.

This system together with two other non-critical associated systems were found to be non-compliant and it was the intention of the Service to have the supplier replace them. Upon replacement, acceptance testing was then to be conducted according to guidance provided by the supplier in the Customer Acceptance Testing manual.

While upgrades for the suite of management systems were to be implemented by the supplier as part of the maintenance contract, the Service had also been diligent in researching and documenting the compliance status of sub-components of these systems. The database which forms the non-compliant back-end of FIRM and the operating system Solaris upon which FIRM resides, were also listed as non-compliant and the required upgrades identified from respective web sites.

Confirmation of compliance had also recently been obtained for the five mainframes that act as hosts for the systems in Burnie, Launceston and Hobart. It should be noted that replication of the systems at each of these locations means that if one system should fail then incident management could be controlled from either of the other locations.

Eight PCs that are used as consoles for the Incident Management Systems were certified as compliant, although in-house testing on these desktops was still to be conducted.

Building and Environmental Systems

A formal plan that addresses building and environmental systems had not been developed, although these systems were included in the database. Consideration had been given to their status however, and several compliance statements obtained.

The Southern, Northern and North West Regional Stations (at which FireComm is located), are provided with back-up generators. While the Audit Office was informed that the generators are tested regularly, supporting documentation was not provided as evidence of this testing.

Water supply for firefighting is an issue for the Service and the Project Manager indicated that this would be addressed via contingency planning. Regular sources of supply will be topped up and discussions held with the Hobart Regional Water Authority to ascertain the status of other sources of supply.

Fire alarms that are internal to the regional stations had not been checked for compliance at the time of the audit, although it was suspected that these were not date dependent.

The compliance status of external fire alarms may be an issue for the Service should the failure mode of non-compliant systems be such that alarms are inappropriately activated. Compliance information on these external alarm systems was yet to be sought by the Service.

The Fire Service did not view other building and environmental systems such as security systems, lifts and air conditioning as critical.

Telecommunications Systems

The Y2K assessment committee was yet to document a formal telecommunications test plan. Nevertheless, compliance certification had been sought and was subsequently provided

for the elements which comprise the Fire Service's various telecommunications networks. Correspondence between the Service and providers had either indicated the extent to which equipment and services were already compliant or highlighted areas where remediation was needed.

Communication within the Service is facilitated through three critical networks - the digital network linking the regional control centres, the paging and radio network and the fire alarm network.

The Radio Command and Control system is used to maintain communication between the regional control centres. Upgrades were required for both the hardware and software of this system and the database indicated that an upgrade tender was under way. Compliance had not been confirmed for the multiplexer and the database indicated that testing was still to be completed. Further testing was also required for the touchscreen PCs of this system as the vendor stated that these terminals were not compliant.

Communication between the command control centres is maintained through the link provided by Telstra. Telstra's web site confirmed that this link should operate before, during and after the date change to the year 2000 without negative impact on functionality. The web site also indicated that other Telstra input into this control system (TASINET, 1-800 and 000) should demonstrate similar functionality.

The supplier of the critical radio paging system proposed that a software specialist carry out tests to determine the status of the system. This testing was yet to be conducted but it was anticipated that non-compliance would be found only with a Unix switch box. Certification had recently been obtained for the critical transmitter and the supplier's web site has showed that the pagers used by the Service are fully compliant since they have no date dependency. The software for the hand-held and mobile (fire truck) radio systems was also designated as compliant by the supplier.

The fire alarm network relies on a combination of commercially provided alarm monitoring equipment and Telstra private lines. Two components of the alarm network have been certified as compliant by their respective suppliers. A third component, however, was not compliant and an upgrade was required. The Telstra web site indicated that the private line should operate before, during and after the date change to the year 2000. The Emergency Reporting Service provided by Telstra to the local alarm network should demonstrate similar functionality.

Other Embedded Systems

A formal test plan addressing other embedded systems had not been developed. However, as the Service has only two critical embedded systems, it would seem reasonable to address these in either the building and environment or the telecommunications plan.

Written confirmation was obtained from respective suppliers of vehicles that embedded systems either had no date-related functionality or that they were Y2K capable. The project database showed that testing was to be completed on the uninterruptable power supply devices.

In-going and Out-going Supply Chain

The issue of supply chain was partially addressed by the draft compliance program. A supply schedule of internal and external testing which was still to be conducted by suppliers, had not been developed.

Stakeholders in the Fire Service's operations have been approached as part of the testing process through a standard letter requesting compliance information. For the most part

stakeholders have outlined their commitment to business continuity and support with regard to their client.

Compliance

An overall compliance plan had not yet been finalised; however, compliance checking through contact with vendors had been the primary means of obtaining compliance information in the first instance. On completion of checking, remediation was to be undertaken which was based upon measures prescribed in the project database. Acceptance testing would then be conducted for critical systems followed by a full end-to-end test in September.

Business Continuity

A comprehensive overarching business continuity plan had not been developed as reliance was placed on the project database for strategic decision-making. It may be worthwhile for the Service to consider developing such a plan so that fundamental aspects of the project could be readily referenced.

Risk Assessment

All critical systems were identified and documented in the project database. Risks were assigned for these systems according to their strategic value and the likely impact of their failure. The majority of non-critical systems were also identified and assessed.

The Risk Assessment Report for the New Zealand Fire Service had been obtained and consideration given to the development of a similar written assessment for the Service. It had been decided that a significant amount of effort would be required to develop such a comprehensive document for little gain and for this reason a project database continued to be relied upon as the risk assessment for the Service. A more succinct written risk assessment risk could, however, be developed as a reference document for the methodology adopted.

As stated at the start of this chapter, definitions of risk categorisations ‘critical’, ’high’, ‘medium’ and ‘low’ had not been explicitly defined by the Fire Service, but rather a common understanding of these terms has been assumed across the Service based upon the extent to which failure of a system would affect the ability of the Service to fulfil the mission statement. Explicit definitions within a document on risk methodology would, however, minimise inconsistencies in the application of these terms.

Contingency Planning

Non-compliant components listed in the project database had been assigned a priority for remediation according to the strategic value and impact upon failure of the item. This is an effective risk minimisation strategy in that it allows the status of critical items undergoing remediation to be readily monitored.

Regarding contingency planning, the organisation is one whose normal functions pivot on responsiveness to critical situations through following Standard Operating Procedures (SOPS). The Service is therefore familiar with the discipline of testing preparedness for emergencies.

The FireComm SOPS are used to address failure of components of the alarm system, FIRM, the paging system, the radio system and the telephone system. Contingency provisions detailed in this document therefore largely address problems arising from component failure

within these systems. Nevertheless, tailoring of this plan for Y2K-specific contingencies was to be undertaken by the Service and it was expected that this would be completed by 30 September 1999.

Criteria for Contingency Mode

Criteria for invoking SOPs are described in the contents section of that document. The contents index summarises the types of problems and failures which may be encountered for each of the critical systems and networks. According to the District Officer for Operations Support, SOPs can be implemented indefinitely and the criterion for revoking the plan is restoration of the failed system.

Criteria for invoking and revoking the Y2K-specific contingencies were yet to be documented.

Staff Training

According to the District Officer, the roles of staff in contingency mode are no different to roles adopted in normal modes of operation because emergency procedures are implemented as part of day-to-day operations. Staff are therefore aware of differences in the management of resources including materials and information systems. Also, a contact list for staff and other emergency services is provided within the Chain of Command section of the FireComm SOPs. Further, staff are exercised in scenario walk-throughs from time to time which focus on improving decision-making skills.

The District Officer also provided the Audit Office with a memo that proposed leave restrictions for key FireComm staff for the period 28 December 1999 to 10 January 2000 to ensure that the maximum number of staff would be available to cope with potential emergencies which may arise as a result of the Y2K date change over.

Contingency Testing

As stated above, the existing FireComm SOPs are implemented on a regular basis and scenarios are practised from time to time depending on the prevailing workload. According to the District Officer, documentation of these exercises was not seen to be necessary because of the changing operational conditions and the need for a high level of flexibility.

It was the intention of the Service to conduct testing on the Y2K-specific plan once it had been completed.

Governance and Reporting

Project staff appeared to be confident that major goals of remediation and contingency planning would be achieved by specified timelines. They also indicated that support in terms of the provision of resources and encouragement had been forthcoming from senior levels within the Service.

The Audit Office is of the opinion that the project has been well managed because of the steady progress which has been made with respect to testing and remediation. Currently, however, this progress is only reported in verbal form to Executive Management on a monthly basis and consideration could be given to the production of regular branch status reports, so that progress with respect to critical tasks can be made more transparent to senior management.

Project Sponsor

The Chief Executive Officer is the project sponsor for the Fire Service and according to the Project Manager he has provided considerable directional support. Since the Project Manager is the Director of Finance Administration he has also had direct input into the allocation of resources.

At the time of the audit, Branch Managers were in the process of completing Y2K project budget estimates for the next financial year and for this reason estimates were not available. The Project Manager indicated that the Service does not expect resourcing of the project to be a major issue. This view was also endorsed by managers who demonstrated confidence that funding requirements would be met.

Reporting

Written reports were not provided to the CEO on a regular basis, but it was the intention of the Project Manager to produce a comprehensive report detailing progress of the project by 30 June 1999. Verbal reporting of issues of concern does occur vertically from Branch Managers to the Project Manager through the Y2K Project Committee meetings. Major issues arising from these meetings are then raised at the senior level by the Project Manager at monthly Executive Management meetings. The meetings held by the Y2K Project Committee have been well minuted and action points documented.

The Project Manager did not consider the regular production of detailed reports to be a priority because to date there have not been any major issues of concern and on-going progress could be gleaned from the project database. Consideration could, however, be given to the development of a database that would allow summarised information on progress in key areas to be recorded by Branch Managers without a significant increase in workload.

The Fire Service has been participating in the Quarterly Budget Committee reporting process and there do not appear to be any major discrepancies between audit findings and responses contained within these reports. One minor discrepancy found was in regard to the responses given in the February and October surveys, which stated that a comprehensive testing plan did address building, environmental, telecommunications, other embedded and supply chain systems. The development of this plan was designated in the response as ‘in progress’. According to the Project Manager, it was his intention to indicate that the testing plan would address these systems rather than indicating that the plan does address them.

The Service is also providing Public Disclosure Statistics on a monthly basis. According to the Project Manager the percentages representing Y2K readiness and contingency planning were not determined using a rigorous quantitative approach, but rather were determined from perceived estimates of effort expended against effort required. Percentages obtained in this way were in agreement with audit findings in as much as compliance checking of critical systems had been completed and remediation of non-compliant systems was proceeding.

However, audit ratings tended to be lower by approximately 10-20%, which may have been because the audit program required documentation (of testing plans, compliance plans and status reports) to be completed, whereas the Fire Service had not viewed these tasks as having a high priority.

The target date of September 1999 for readiness and planning was chosen to allow for the completion of all acceptance testing and contingency planning before end-to-end testing was conducted. The project and planning schedules were designated as being on schedule and while the project database indicated that remediation measures had been determined, detailed schedules of remediation for each branch had not been developed. As a

consequence, it was difficult for the Audit Office to accurately assess the statement that the project was on schedule for all key services. It should be noted, however, that the impression gained from interviews conducted with managers was that planned upgrades would be implemented without significant delays.

Timelines

The preliminary tasks of risk assessment and compliance checking have been completed. It was anticipated that all remediation and contingency planning would be completed by 30 September 1999 when end-to-end testing will be conducted.

The development of detailed project schedules is required to provide confidence that this milestone can be achieved.

Information Gathering

Information gathering on the part of the Service had been extensive with the Project Manager participating in several Y2K forums. These included a national teleconference organised by the Australasian Fire Authorities Council (AFAC) and project manager forums organised by the Whole of Government Projects Unit.

External quality assurance had not been sought for the whole project, however, the Manager of Communications indicated his intention to seek quality assurance from a consultant for the telecommunications component of the project.

Also, information on peer projects had been obtained from the New South Wales Rural Fire Service and the New Zealand Fire Service.

Awareness-Raising Activities

The Y2K Project Committee, comprising the project manager and branch managers, meets fortnightly to discuss the progress of the project. Minutes of these meetings had been documented and circulated.

A newsletter explaining the nature of the Y2K Problem, as well as requesting staff input into the project, had been circulated throughout the Service. End users of systems and staff affected by contingency plans, however, were yet to be informed of any changed roles and modes of operation.

More recently the release of Public Disclosure Statistics and the assignment of a media officer had provided a mechanism for the Service to raise public awareness of the project.

Conclusion

The Audit Office considers that the Tasmania Fire Service project is well under way with key aspects of the project being suitably prioritised. Management of the remediation of critical systems has been delegated to appropriate, capable staff and steady progress was being made in this respect.

The development of plans which detail testing and remediation guidelines, processes and schedules for all aspects of the project could assist managers to coordinate tasks more effectively.

Auditee Update

'The Tasmania Fire Service has made considerable advances in its endeavours to ensure Year 2000 (Y2K) compliance since the performance audit in April 1999. All TFS file servers and associated critical operating systems and database management systems have been upgraded and are now Y2K compliant. The TFS recently received Y2K compliant versions of the operational software along with comprehensive Y2K certification documentation. Acceptance testing of the software is in progress and the TFS is on line to have end-to-end testing completed by the end of September 1999.'

HOBART CITY COUNCIL

The Audit Office carried out a review of Hobart City Council during April and May 1999.

Testing

Hobart City Council developed a project plan in the form of a Gantt chart with targeted start and finish dates for various aspects of the Y2K project. A formal plan for physical testing conducted by the Council was yet to be developed for each of the key areas, although much of the material needed to construct one was readily available.

Risk assessments were undertaken by the Council in August 1998 with four areas classified as critical to its operations, namely water supply, sewerage, the Tattersalls Hobart Aquatic Centre (THAC) and information services. Although clearly stated and replicable definitions of levels of criticality such as would be afforded by scales or matrices of risks were not used, Council Y2K project staff had a sound understanding of the concept as it applied to Council's operations.

An inventory of relevant plant, equipment and software was created from asset register files and down-loaded onto spreadsheets, which were produced for the various divisions within council. Managers and their staff rated individual items so that the completed spreadsheets provided the basis for subsequent follow up action. Any items that had not been listed were added as necessary. A clear indication of the potential for Y2K problems for all affected items was readily provided by this easy-to-use system.

The Council's Corporate Management Team (CMT), which is comprised of the General Manager and five directors, set the goal that all testing should have been completed by the end of June 1999.

IT Systems

As stated above, Hobart City Council had not yet produced a formal test plan. As well, a separate plan had not been developed specifically for IT, although much work had been done in respect of the Local Government Information System (LGIS). This system is the principal program element of Hobart City Council's IT environment and is used for a diverse range of accounting and property functions, including the general ledger, payroll, stores accounting, parking register, rates etc. It is also crucial as the source of day-to-day management information and data used for long-term planning. The decision to undertake remediation, rather than replacement, was based upon a well-documented risk assessment. The determination of the criticality of components was supported by defined risk categories specified in Appendix 2 of the Project Execution Plan. The highest or critical level of risk (Risk 1), should be applied to:

> 'an operational system, the short term failure of which or the provision of incorrect information may lead to death, injury or serious loss of property.'

The manager of IT systems explained that Hobart City Council has a commitment to extensive pre-release testing of LGIS in order to obtain Y2K trouble-free operations. Updating and testing of LGIS had involved joint efforts by the supplier and Council, which have worked in tandem with a users group of other interested Tasmanian and interstate councils. A spare Virtual Address extension (minicomputer server) (VAX) was leased as an off-line test facility to enable trials to be safely conducted using actual data taken from the live environment. At the time of the audit Beta testing was continuing, with 30 June 1999 envisaged as the end date for testing.

Compliance statements had been obtained from vendors via the Internet for Council's network hardware and software. Where necessary non-compliant items were being upgraded or replaced.

A proprietary testing package had been acquired that examined and checked the Basic Input Output System (BIOS), applications and data files on each PC. Appropriate remedial action was to be developed from the reports generated in respect of each machine as a result of testing.

Building and Environmental Systems

Based on Hobart City Council's risk assessment, the only critical building and environmental systems were those associated with water, sewerage, THAC and IT. Council approached suppliers or contractors to ascertain possible Y2K implications in respect of fire alarm, security and other services fitted in the buildings affected. The ultimate aim was for testing to be completed by 30 June 1999 and for warranties to be obtained in respect of high-risk equipment in these premises. Depending on the outcome of test results and the degree of certification provided by suppliers Council anticipated that additional testing may be scheduled. Although the process was progressing, no formal test plan existed for building and environmental systems.

Telecommunications Systems

Hobart City Council did not identify telecommunications as critical and was relying on compliance certification given by Telstra and Optus as the suppliers of the various products and services in use. Regardless of the criticality rating, suppliers of telecommunications equipment (eg PABXs) had been contacted to ascertain either the degree of Y2K compliance or actions needed to ensure upgrading to achieve compliant status.

Data communications, however, form part of the IT network which was rated as critical and so this component fell within the scope of the audit. Data network communications were via Ethernet with outposted locations connected by either council-owned microwave radio (Clearys Gate and THAC) or optical fibre (Council Centre) and dial-up facilities.

Compliance certification had been obtained from the respective service providers in respect of the telecommunications products.

Although telecommunications were not assigned a critical rating, contingencies existed to enable on-going communications with staff operating or monitoring critical systems such as water or sewerage. For example, in the event of failure of the in-house telephone network two-way radio could be used to communicate with council staff in the field who could be directed to strategically sensitive sites.

Other Embedded Systems

For Hobart City Council the water, sewerage and THAC systems were the main critical areas for embedded technology. Hobart's water and sewerage systems are to some extent shielded from Y2K vulnerability because of two factors, namely older generation plant that is mainly electro-mechanical and lacking in programmable logic controllers (PLC), combined with the city's topography that provides a large measure of gravity feed for both systems. Water and sewerage systems do nonetheless contain PLCs.

To deal first with sewerage, there are two wastewater treatment plants (WWTPs) to handle Hobart's effluents. The older of the two WWTPs is at Macquarie Point and it processes outflows from the city area, while the newer plant at Selfs Point processes material from Sandy Bay and New Town. The city and New Town catchment areas rely on gravity feed to

their respective treatment plants, whereas two pump stations are needed to send wastes from the Sandy Bay area to Selfs Point.

Selfs Point has a backup electricity supply in the form of a diesel generator so that it could continue to function in the absence of mains power. There is, however, no such facility at either of the intermediate pump stations that bring effluents from Sandy Bay. In the event of prolonged power outages this material would have to be released into the Derwent River in untreated form. In the case of power failure the Macquarie Point plant would be rendered inoperative and raw sewage would bypass the plant and directly enter the river. Due to its design, though, this plant would be able to resume its normal operation within a few minutes of power being restored.

Control and treatment equipment fitted with PLCs was subject to initial audit by subcontractors appointed by the manufacturers. Similar software was used at both WWTPs and Y2K upgrades were planned at the two locations after which rollover tests were to be carried out. In the event of failure of computer control equipment both plants have the facility to be run manually.

Hobart is dependent for its water supply on the Hobart Regional Water Authority. Reticulation within the area controlled by Council relies on a combination of gravity feed and pump stations. Hilltop reservoirs that are common in a number of suburbs will be filled prior to January 2000 to provide a strategic water reserve ensuring a partial 'buffer' in the event of upstream problems or power failure. Within the Council's water supply system there are a number of pump stations which, although electrically powered, do not incorporate PLC technology.

The manufacturers were approached for information regarding the Y2K status of the electronic control systems used in vehicles in the Council's fleet and certification has been obtained from them.

At THAC there are a number of devices containing embedded technology: water and air temperature control equipment and water purification and cleansing plant. Additionally, a diesel stand-by generator is available to supply electricity in the event of power outages. This would permit the continued operation of water filtration and recirculation as well as lighting. Compliance testing of the various items of plant at THAC had been commissioned from the relevant suppliers and was in progress during the audit.

In-going and Out-going Supply Chain

Hobart City Council's major customers have been contacted and advised of the Council's initiatives in relation to Y2K issues. Testing of the in-going and out-going supply systems had mainly been done by suppliers and certification either had been or would be obtained from them.

Compliance

To aid in the process of compliance testing, certificates originally derived from the British Standard for Y2K compliance were used as the basis for some Council testing. Date integrity, discrimination, process, order, calculation and leap year were defined on the certificate which also outlined the scope, objectives, guidance and expected scenarios for each of the above-mentioned criteria. These certificates were forwarded to suppliers or manufacturers. Components were either endorsed as compliant or non-compliant except for those that have no date dependency which were indicated as 'not applicable'.

IT Systems

In view of extensive work done to date on LGIS and PC workstations it was estimated by the Council that 75% of compliance checking had been completed.

Building and Environmental Systems

Building and environmental systems were estimated to have achieved 50% compliance, which in view of the amount of work yet to be done was regarded as being on target.

Telecommunication Systems

As previously mentioned Hobart City Council is relying on work being done by Telstra and Optus and viewed compliance telecommunications as just 10% complete.

Other Embedded Systems

As an area that has a number of critical systems that are Y2K vulnerable a large amount of effort has been devoted to compliance testing in the field of embedded technology. Compliance status of PLC-enabled equipment is continuing and the task was viewed as 50% complete.

In-going and Out-going Supply Chain

The Hobart City Council has considered external relationships. In contacting stakeholders the Council used debtor and creditor files to generate names and addresses for a complete list of all business contacts to be included in the mailing list. Staff were also asked to nominate any outside parties with whom they had business dealings so that they could be included in mail-outs regarding Y2K issues.

Business Continuity

Hobart City Council developed a Project Plan that detailed the objectives and milestones of the Y2K project. This plan outlined a number of steps from risk identification and inventory preparation through to testing and remediation. As well, it made provision for the preparation of business continuity plans in all of the areas rated as critical.

Risk Assessment

Assessments of risk and setting of priorities were highlighted early in the Project Plan and actioned between August 1998 and February 1999. Risk categories were defined, on the basis of likelihood and expected consequences of possible failure, for application to key areas as an aid to their on-going testing and remediation.

The method of inventory compilation described in the section on testing provided a ready mechanism for the assignment of risk to Council plant and equipment.

Contingency Planning

Hobart City Council's business continuity was to be based upon activation of the contingency plans that were incomplete at the time of the audit. It was envisaged that the Council's on-going involvement in disaster and emergency planning activities would provide a suitable framework for the development of contingency plans.

Among existing plans that would provide a basis for contingency planning, the Audit Office examined two in particular: the Hobart Emergency Management Plan (Issue 3, April 1996) and a draft of the Incident Management Plan for the WWTPs (April 1999).

The Hobart Emergency Management Plan was issued under the authority of the State Emergency Services (SES). It is a generic type of document and rather than spelling out in detail how particular emergencies would be handled in a step-by-step method it explains how the Council would respond to a range of emergencies in conjunction with other essential services. It is this coordinated approach with other organisations or agencies (together with a description of their respective roles and responsibilities) that is specified within the plan. Appendices detail likely scenarios and identify the relevant contact points within each of the lead combat authorities.

The Incident Management Plan (IMP) outlines operational response capabilities aimed at preventing or minimising impacts of unforeseen events at the WWTPs. In turn, a range of other documents and procedures covering matters such as safe operating guidelines, chlorine leaks and emergency evacuation plans supports the IMP. With regard to recent activities related to potential Y2K Problems, the Council had to respond to an emergency chlorine leak at Selfs Point earlier this year. As a result of a post-incident follow-up refinements were made to the operating procedures and IMP.

In addition to the emergency contact lists contained in each of the plans referred to the Council has an after hours duty roster that is regularly updated.

Consideration was given to other aspects of contingency planning and Council's Civic Solutions division was involved in desktop emergency management activities. Other contingency provisions considered by Council have included stockpiling (eg water reserves in reservoirs), revocation of holiday leave for key personnel or bringing forward or delaying routine tasks to more evenly spread workloads and minimise risks at the crucial dates.

Hobart City Council was also considering setting up a help-line to provide practical assistance to small businesses that may be adversely affected by limited duration, localised failure of services that could threaten their survival in the short term. Such assistance would be available subject to the Council's own needs but it could, for instance, take the form of assistance with transport services, technical advice or the loan of spare equipment.

Criteria for Contingency Mode

The Council intended to develop Y2K criteria for the full contingency plan. In its normal role as a community service provider the Council is often called upon to respond to emergency situations (eg bushfires, land gales and flooding) and the experience gained in these crises had been incorporated in revisions and refinements of emergency plans. The adaptation of these plans for Y2K contingency planning should not be a time-consuming task, however, the process was still continuing and had yet to be documented in full, with a target date for completion of 1 November 1999.

Staff Training

Council staff already have some experience of operating in a contingency mode since some activities undertaken by the Council are in response to unanticipated incidents or equipment failures as outlined above.

As a further contingency measure extra staff may bolster the number of key staff already designated for after-hours call out in the after hours duty roster for the period from late December 1999 to early January 2000. This proposal would be supported by a temporary suspension of holidays for those who are affected.

Contingency Testing

The fact that the Council is required to regularly deal with unforeseen incidents, combined with a willingness to improve existing techniques as a result of these events, means that there is regular testing and feedback of emergency procedures.

Governance

Governance and reporting for this project appears to be satisfactory. Resourcing, whether in the form of funds or secondment of staff as necessary had been made available to keep the project on track. Staff interviewed by the Audit Office were comfortable with the direction and organisation of the project and believed that milestones would be achieved.

Project Sponsor

The project's sponsor is the Director of Corporate Services (also a member of the CMT) who reports to the General Manager. The Council also has an active Y2K committee with representatives drawn from each division.

Although the Hobart City Council had not prepared a separate Y2K budget, consideration had been given to levels of resourcing needed to attain the goals of the project. It was proposed that the necessary expenditure would be accommodated within existing budgets and that re-scheduling of expenditure programs would take place to meet any urgent, unanticipated outlays.

Quality assurance had not been specifically sought for the Y2K project, however, the Council does have a culture of continual improvement and has achieved quality certification in some of its divisions. During 1999 the General Manager has championed the theme of quality management.

Reporting

There are regular lines of reporting between the Y2K project manager and the sponsor. The project manager has submitted written progress reports fortnightly to the CMT since January 1999. As well, he had occasionally attended council meetings to provide briefings on Y2K issues.

Within the IT environment there is a user group of Councils that report on developments regarding testing and upgrading of LGIS.

The Council has been party to the monthly Public Disclosure Statistics process. The project manager explained that percentages submitted by Council could not be supported by a rigorous, documented approach but instead were based on estimated effort expended to date and that required to finalise a task.

The Statistics reviewed in this audit were those published for March 1999. As a result of discussions and documentation examined, the Audit Office formed the opinion that the Council's reported percentages for readiness were rather high given that the critical areas still had considerable work remaining to be done. Nevertheless, the target date of 30 June for readiness seemed likely to be met as work on the Y2K project was progressing smoothly.

Existing emergency plans provide a basis for the development of contingency plans and it was the Audit Office's opinion that work was advancing satisfactorily. The contingency planning target date nominated in the Statistics was 1 November 1999, which should allow adequate compliance testing to be undertaken.

Timelines

As mentioned previously, a Y2K project plan was developed and timelines established on the project schedule. Inventories and risk assessments were completed and documented on schedule. Completion of testing was due on 30 June 1999 and it seemed likely that this was an achievable goal.

Information Gathering

Information has been gathered from a range of sources including the Internet, peers and industry (eg Tasmanian Electricity Supply Industries, the LGIS users group, The Mercury). Also, a Council representative attended a conference on Y2K legal issues in Hobart in October last year that provided a useful opportunity to exchange ideas with peers. A similar opportunity, also in October 1998, was provided by a Gartner Group presentation that focused on Y2K risk assessment and planning.

Awareness-Raising Activities

Hobart City Council has been diligent with regard to awareness-raising activities which have encompassed presentations made to all staff, memoranda from the General Manager and briefing sessions for sub-managers and staff.

Conclusion

At the time of the audit Hobart City Council's Y2K project appeared to have been adequately managed. The Council should be in a sound position to manage incidents that may arise, provided that the remaining testing, documentation and development of the contingency plan proceeds according to schedule.

Auditee Update

'The Year 2000 Performance Audit was carried out in April and May 1999 and no doubt it is recognised that great strides have been achieved by the Hobart City Council since that time. The substantial progress made is amply evidenced by Council's monthly report to the Whole of Government Working Group.

The Council's major focus now is on "business continuity planning", with particular emphasis on identifying our business processes/activities and preparing contingency plans in the event that certain elements may potentially be taken out of service or be unavailable due to the Y2K Problem.

The Council's approach to the Year 2000 Problem started formally in October 1997 and has been proactive to ensure there is an understanding of the consequences and strategies in place to ensure compliance.

The Hobart City Council is confident that it has undertaken all reasonable measures to ensure that its services are "Y2K ready"'.

LAUNCESTON CITY COUNCIL

The Audit Office carried out a review of the Launceston City Council (LCC) during May 1999.

Testing

The Council had displayed a considered, systematic approach to Y2K issues and it was evident that the project is being well managed. A schedule was drawn up listing targeted start and finish dates of various aspects of the project, together with the names of the people responsible to progress particular issues. LCC had not yet documented a formal Y2K testing plan. Much of the material required to document a testing plan, however, had been completed and was available. Minimal effort would be required to incorporate the material in a formal plan.

Risk assessments were undertaken by the Council during the first phase of the project, which was completed at the end of September 1998. Critical operations or areas were then identified according to ratings of probability and seriousness. These terms were themselves defined in an impact matrix, thus allowing consistent and replicable standards to be applied. The highest priority was assigned in those cases where a system was viewed as having high probability (susceptible to failure which will require extensive repair/resources before a basic device can be provided) combined with high seriousness (vital function and its continued unavailability could cause loss of life or property and serious impact on the business sector).

In order to produce an inventory, data was down-loaded from asset register files to a database and equipment details were added to it after a visual assessment (crosscheck) of each working area. This information was then reviewed to assess the vulnerability of all individual items of plant and equipment owned and operated across the entire Council. The database was an effective management tool since it cross-referenced files containing relevant correspondence and compliance certification statements from suppliers and contractors. A clear indication of the state of Y2K compliance of all affected items was readily provided by this easy-to-use system.

Compliance checking was proceeding with respect to IT, telecommunications, building and environmental systems, other embedded systems and the in-going and out-going supply chain. A formal plan for physical testing conducted by the Council was yet to be developed for each of the key areas.

IT Systems

As stated above, Launceston City Council had not yet produced a formal test plan. A separate Concept Plan, however, was developed specifically for IT and encompassed a wide range of project management objectives and deadlines.

As a result of the risk assessment process IT was one of the areas assigned the highest rating of Y2K criticality. Components falling into this critical category include all computer hardware, networking software and the Council's corporate business systems software.

The system currently used for a wide range of these functions had been scheduled for replacement later this year. A tender for the supply of necessary software and hardware, in which Y2K compliance was clearly stated as a condition, closed in February 1999. Tender evaluation was under way, with the likelihood that the new system would be installed and operating before the end of 1999. The new system may be configured from a number of smaller off-the-shelf packages spanning the range of functions presently included in the current system. As a fall back position Y2K-compliant releases of the current system have been installed.

Compliance statements had been obtained from vendors off the Internet for network hardware and software. PC BIOSs were tested by means of a share-ware tool also obtained from the Internet. Testing of applications, data files and operating systems were still in progress at the time of audit and Launceston City Council was considering obtaining a Y2K PC test package for this task.

Building and Environmental Systems

Launceston City Council's inventory contained 165 building and environment components that were considered to be in the critical group. With the exception of one item (1 out of 25 internal lighting systems) all 165 had been checked by mid-April 1999. Only one system was found to be non-compliant (a security system for the Town Hall) and was being upgraded.

Compliance certification had been sought in respect of all items. Where suppliers' statements indicated that equipment was Y2K compliant but date dependent the Council intended to conduct its own tests.

In the event of a crisis the Town Hall annexe building will be used as an emergency operations control centre. A stand-by diesel generator was available to provide emergency power should it be necessary. The generator itself had been checked but Audit did not sight a log sheet to confirm this.

Telecommunications Systems

Two areas of the Council's telecommunications system had been identified as critical, namely Telstra data links and in-house telephones, which are provided by TASINET. Data communications were treated as part of IT, with other non-critical telecommunications components ranked in the following order of priority: two-way radio, e-mail, microwave links, land lines and mobile telephones.

Compliance certification had been obtained from the respective service providers of these telecommunications products.

For a number of the components cited above, contingency plans already existed to ensure the continued operation of systems. For example, in the event of failure of the in-house telephone network two-way radio could be used to communicate with council staff in the field. Also, in the event of failure of the supply of electricity the back-up generator could provide an alternative supply for the Town Hall annexe building.

Other Embedded Systems

For Launceston City Council the critical areas for embedded systems were found in the water and sewerage systems. The city's water and sewerage systems were to some extent protected from Y2K vulnerability because of two factors: older generation plant that is mainly electro-mechanical and lacking in programmable logic controllers (PLC), and Launceston's topography that provides a degree of gravity feed for both systems. Water and sewerage systems do, none-the-less, contain some items of embedded technology.

Compliance certification had been obtained for PLCs in the sewerage system and roll over tests conducted on the pumping station at the Gorge cliff grounds. So far as embedded technology at the Ti-Tree Bend wastewater treatment plant was concerned, a failure of the secondary computer in February provided an opportunity to gauge the plant's operation under emergency operations. At that time it was indicated that the primary control system would switch to manual in the event of a PLC crash.

It was also planned to provide a diesel generator at the Ti-Tree Bend plant to allow the continued operation of two (out of four) screw pumps that feed waste water from sewer

lines into primary treatment tanks, from where gravity will enable its continued passage through to downstream tanks. In the event of power failure, continued operation of the screw pumps is essential because they would allow the plant to continue functioning without deterioration in effluent quality for several hours.

Launceston is dependent for its water supply on Esk Water. Reticulation within the Council's area is a combination of gravity feed and pump stations. Hilltop reservoirs will be filled prior to January 2000, ensuring a partial 'buffer' in the event of upstream problems or power failure. Within the water supply system just one pump station, Lower Brougham Street, incorporates PLC technology. Although certified as compliant the Council was conducting a range of tests, including an 'on and off' test which mirrors an actual scenario in the case of power loss and subsequent re-starting. A telemetry system is used for overall management of water reticulation but it does not have the facility to open or close valves, so its operation is not critical to the supply of water.

Manufacturers have been approached for information regarding the status of electronic control systems of vehicles in the Council's fleet. Certification had been obtained and was made available to Audit.

Compliance certification had also been obtained for the gas detection unit at the Council swimming pool, which is used as an alarm system in the event of leakage from chlorine stocks used for water treatment at the facility.

In-going and Out-going Supply Chain

Launceston City Council's major customers were contacted in August 1998 and advised of the Council's initiatives in relation to Y2K issues. For the most part, testing of the foregoing systems had been done by the supplier and certification obtained.

Compliance

The approach to compliance favoured by Launceston City Council was based on a commercially available methodology that has been a regular part of the Council's management processes since the late 1980s. The Launceston Y2K project team believed that compliance testing brings with it the risk of triggering failure of critical systems and that it should not be commenced without a contingency plan first being in place. Subsequently, if compliance testing does cause failure or reduced levels of operation remediation could be quickly initiated.

Compliance plans for each of the key areas were being developed using this methodology that imposed a particular rigour.

Existing plans that were already familiar to council staff (in some cases through previous exercises), such as the Municipal Emergency Management Plan (MEM), Disaster Recovery Plan and the Incident Management Plan (IMP), provided a framework within which Y2K contingencies were being developed. Details of after-hour responsibilities and contact personnel in the council and other agencies were contained within the plan.

In relation to IT systems, building and environmental systems, telecommunication systems and other embedded systems the plan viewed by the Audit Office indicated that compliance testing of critical systems should be completed for each of the system areas listed by 31 July 1999.

Business Continuity

A Project Concept Plan was drawn up in which a number of issues were covered including background, a general overview, major threats to success, as well as the five phases of the project. The review phases clearly set out major deliverables, key objectives, responsibilities and timings.

Risk Assessment

Risk identification and setting of priorities were actioned during phase one of the project schedule and completed in October 1998. Risk categories were defined and applied to key areas to aid in the development of their testing and remediation programs. The use of clearly defined terms allowed a consistent approach.

Contingency planning

Business continuity is based upon activation of the contingency plan, which was planned for completion by the end of July 1999, and is dealt with under phase four of Launceston's Y2K Business Continuity Project. This plan draws considerably from the Council's on-going involvement in disaster and emergency planning activities over a number of years and was being developed within the previously mentioned (Kepner-Tregoe Potential Problem Analysis) methodology.

Launceston City Council's IMP outlined operational response capabilities that were aimed at preventing or minimising impacts of unforeseen events. In turn the IMP slotted into the broader MEM coordinated by SES and integrated with plans of other agencies. With regard to recent activities related to potential Y2K Problems the Council had participated in Northern Region Disaster Planning Group workshops organised by SES.

While the IMP impacted on the management structure and reporting mechanism from all incidents involving the Council it did not address the operational management of various incidents. Rather, it formed the basis on which other more detailed and specific plans and procedures could be implemented (for instance the Council's Flood Warning Procedure). Significantly, the IMP had checklists of Site Managers and Incident Managers who were responsible for various emergency situations.

In its normal role as a community service provider the Council is often called upon to respond to emergency situations (eg Hobblers Bridge in 1996) and the experience gained in these crises have been incorporated in subsequent revisions and refinements of emergency plans. The adaptation of these plans for Y2K contingency planning was taking shape, however, the process in its entirety had yet to be documented in full.

Criteria for Contingency Mode

The Council intended to develop Y2K criteria for the full contingency plan and given the degree of organisation demonstrated and progress achieved at the date of the audit, it would be reasonable to expect that the final milestone of 31 July 1999 for the completion of all contingency planning would be achieved. Worksheets used for development of the contingency plan were examined and indicated that criteria for invoking, revoking and functioning in a changed mode of operation were in the process of being documented.

Staff Training

Council staff already had some experience of operating in a contingency mode as some activities undertaken by the Council are in response to unanticipated incidents or equipment

failures. In addition, testing of the IMP and MEM is regularly carried out with information gained at de-briefings used to refine these plans.

As a further contingency measure extra staff, particularly managers, may bolster the number of key staff already designated for after-hours call out in the IMP for the period from late December 1999 to early January 2000. This proposal would be supported by a postponement of holidays for those who are affected.

Contingency Testing

The regularity with which the Council handles unforeseen incidents, combined with a willingness to learn from these events, showed that there was regular testing and review of emergency procedures.

Governance

Governance and reporting for this project appeared to be of a high standard. All staff interviewed were comfortable with the direction and organisation of the project and confident that milestones would be achieved.

Project Sponsor

The project sponsor is the General Manager. Although a separate Y2K budget has not been prepared, consideration had been given to levels of resourcing needed to ensure that the project's objectives are met. It was anticipated that the necessary expenditure would be accommodated within existing budgets. Re-scheduling of expenditure programs would take place to meet any urgent, unanticipated outlays.

Reporting

The Y2K project manager has been reporting to Executive Officers Meetings on a needs basis since the inception of the project. These reports have been thorough, clear and concise in their documentation of issues of concern. Progress and executive reports have also been furnished to the General Manager. Reports and briefings are also prepared for Council.

Members of the project team have met often, with frequency depending on the overall progress of issues. These same team members have been convening meetings or information sessions for staff in their respective work locations. Quality assurance of reporting and other aspects of the project has been strongly supported by having three accredited International Standards Organisations (ISO) 9001 internal auditors on the project team. On balance, most reporting has been done monthly.

The Council had been party to the monthly Public Disclosure Statistics process but has not supplied data since the March report, believing that the statistics do not accurately depict the Council's state of Y2K preparedness. The Project Manager explained that readiness percentages submitted by Council were not the result of a rigorous quantitative approach but instead were based on estimated effort expended to date and that required to finalise a task. All of the Council's key services were included, but these did not necessarily align with services defined as critical for the purposes of this report. As the services were not weighted, however, the figures published (arrived at by averaging the individual percentages applying to each Council service) did not accurately represent the amount of effort expended.

As a result of discussions and documentation examined, the Audit Office formed the opinion that the percentages for readiness published in the March Public Disclosure Statistics were

either correct or understated. In addition, the Audit Office's view of work done to date was less conservative than the Council's own assessment.

An example of the Council's conservative approach to statistics is provided by information published in relation to contingency planning that indicated that no work had been done to create back-up plans. The Council regarded contingency planning as the fourth phase of a five-part process and believed that until all parts were completed it could not be given an interim assessment. The Audit Office's opinion was that work was well advanced (and supported by existing emergency plans) and that in this particular case an evaluation of greater than 50% could be justified.

The contingency planning target date had been moved out from 30 June to 31 July due to some time slippage in the testing phase. This development was not of great concern because of work done so far and the impression gained from the Project Manager was that the new target would be met.

Timelines

Timelines for each of the review phases were prepared on the project schedule. Inventories and risk assessments (phases 1 and 2 respectively) were completed and documented on schedule. Some minor time slippage occurred under the third phase (compliance testing), but the rigorous approach taken by the Council would indicate that this was not of concern.

Completion of testing was due on 31 July 1999, and at the time of the audit it appeared to be achievable.

Information Gathering

Information has been gathered from a range of sources including the Internet and industry (eg Tasmanian Electricity Supply Industries, BHP). Contact with State Government agencies, as in the combined activities and meetings with SES previously mentioned, has been a means of information gathering. Also, the Project Manager and an engineer attended a conference for Y2K contingency planning last year, which provided a useful opportunity to exchange ideas with peers. Quality assurance has been sought internally in as much as the project team had its own complement of quality assurance managers.

Awareness-Raising Activities

Launceston City Council has been diligent with regard to awareness-raising activities, which have encompassed presentations for managers, memoranda from the general manager, briefing sessions for sub-managers and staff newsletters. Meetings of project team staff have been convened fortnightly.

Conclusion

At the time of the audit Launceston City Council's Y2K project appeared to have been effectively managed. The Council should be in a sound position to manage incidents that may arise from the problem, provided that the remaining testing and development of the contingency plan proceeds according to schedule.

HOSPITAL SERVICES

The Audit Office carried out a review of the Hospital Services Division of DHHS during late April to early May 1999 at the Royal Hobart Hospital (RHH) as a representative example of a Tasmanian public hospital.

Testing

The DHHS project plan is at broad level and requires each business unit to exercise their initiative in deciding how and when to test. Neither a definitive formal test plan outlining testing and compliance requirements nor a project schedule had been developed for the RHH at the time of the audit. A number of systems were contracted out, but systems utilised by medical imaging, pathology and pharmacy were managed in-house. The contracted services included several IT, biomedical and building systems.

IT Systems

The contractor had developed a list of 'Year 2000-ready' modules that were used to monitor patient admissions, discharge, transfer, medical records and billing information. The modules were considered to be critical for operational continuity and the RHH was therefore working towards implementing the appropriate Y2K patches to ensure compliance.

The IT services section within DHHS had arranged a quotation for a desktop audit of the RHH. An inventory was also being prepared of the networking infrastructure managed by IT services and the target date for completion was 31 May 1999. The strategy for testing and remediation of this infrastructure was still to be determined.

Building and Environmental Systems

A number of building systems had been identified as critical by the information systems manager, namely the fire alarm, sprinkler, lifts, air conditioning, water supply and lighting systems. It was explained to the Audit Office that the contractor responsible for managing these systems was developing an inventory of building items and it was expected that testing would be completed by 31 May 1999. The RHH had a back-up generator that serviced the hospital and documentation indicated that it was tested frequently.

Telecommunications Systems

All Divisions of DHHS had recently been asked to submit an inventory of telecommunications equipment and the RHH had begun work on this task. Once collated this inventory would then be transferred to Telstra where the compliance status of equipment could be ascertained from an extensive database. Options for upgrade or replacement would then be determined according to the designated failure mode of non-compliant critical equipment.

Other Embedded Systems

The Information Systems Manager had begun to develop a comprehensive list from existing data of all hospital biomedical equipment used in critical processes. The status of items on this list was being determined from a range of sources, including the NSW Y2K web site biomedical database. Vendors managed a large proportion of hospital biomedical equipment and an inventory of these items had been supplied. As with the building systems, vendor testing had recently begun and was supposed to be completed by 31 May 1999. All critical equipment within the departments of Pharmacy, Pathology and Medical Imaging, was jointly

managed by the hospital and vendors and therefore some responsibility for attainment of compliance rested with the hospital.

In-going and Out-going Supply Chain

Major suppliers of hospital software and equipment had been contacted but, as noted in the embedded systems section, Y2K compliance was still to be sought from a number of vendors of critical items.

Compliance

A formal compliance plan had not been developed. It was the intention of the hospital, though, to have all non-compliant systems meet the definition of compliance proposed by Standards Australia. Quality checking had been undertaken in as much as Monash University had examined contractor-tested findings, and some joint validation of biomedical certification had begun to occur through crosschecking of compliance information provided by the Launceston General Hospital biomedical database. End-to-end testing was not to be conducted but contractors were to employ partial acceptance testing for some systems.

At the time of the audit remediation had not been completed for any non-compliant critical systems although, as explained in the section on testing, measures for remediation had been proposed for a number of systems. It was anticipated that all remediation would be completed by 30 September 1999, but this is reliant on vendor timeframes.

Business Continuity

A project plan for DHHS detailed the objectives and scope of the Y2K project for the Department. These included full documentation of all aspects of Y2K work through to the categorisation of key business activities and the development of contingency plans.

A specific project plan of this type had not been developed for the hospital and, as a result, the Audit Office considered that a coordinated approach was lacking.

Risk Assessment

A matrix linking critical processes to departments had been developed and also items related to key business processes including critical inputs and outputs had been identified by all hospital departments. These items were still, however, to be collated into a comprehensive risk assessment that concisely ranked criticality. A draft risk analysis of IT infrastructure was in the process of being developed at the time of the audit.

Contingency Planning

A comprehensive hospital disaster plan detailed contingency modes of operation for all departments. This plan addressed the preparedness of the RHH to mount an external emergency response as the emergency receiving hospital within the Acute Care Program. Command, control, coordination and notification procedures were clearly outlined within this document.

A contingency framework titled Critical Operations Standing Operating Procedures (COSOPS) had been obtained from the New South Wales Hospital Service. Each hospital department intended to complete the framework by 30 September 1999 and guidelines for completion had been developed and distributed. Proposed contingencies included the delaying of elective surgery, the revoking of leave for staff and the stockpiling of medical supplies.

A contingency plan for the Department of Emergency Medicine had been developed for the primary computer system module's downtime. This plan addressed procedures to be adopted in the event of a system crash, planned downtime and the consequential re-entering of data. A general IT contingency plan was also in the process of being developed.

Criteria for Contingency Mode

The disaster plan examined by the Audit Office contained criteria for invoking, revoking and functioning in a changed mode of operation.

Staff Training

Hospital staff engaged in mock disaster scenarios as a requirement for the Australian Council of Healthcare Standards accreditation process. It was intended that staff would be fully trained in Y2K contingencies towards the end of 1999.

Contingency Testing

An operational report and debrief of an exercise conducted at the Hobart International Terminal was provided to the Audit Office as evidence of the testing of the disaster plan. Another tabletop disaster exercise was planned for September 1999.

Test results for the emergency diesel generator indicated that it was tested on a weekly basis.

Governance

Project Sponsor

The Deputy Secretary of DHHS is the project sponsor and according to the interviewees he had assisted with raising the profile of the project across divisions. The Information Systems Manager was appointed as the Y2K project coordinator for the hospital in early April 1999 and the Audit Office considered this to be relatively late in the process. This appointment, as well as that of a part-time assistant, make up the 1.5 FTEs that had been specifically allocated for the management of the hospital project. The estimated proposed cost for 1999-2000 was $152 000. This total did not include the cost of remediation of any biomedical equipment since this additional amount was still to be determined. The Project Manager was advised by the Senior Business Advisor that the Funding Review Committee had concluded there was no capacity to provide additional funding for the Y2K project as a new initiative. Accordingly Y2K costs were to be funded by Divisions.

Reporting

The Y2K steering committee provides written reports on a monthly basis to the project sponsor on the progress of DHHS as a whole. The Business Risk Manager for the Hospital and Ambulance Service is a member of this committee and has reported verbally to the committee on the progress of the Hospital.

Information on the status of hospital biomedical equipment was not found in the steering committee reports and the auditee advised that apart from the public disclosure statistics, written reports on the progress of the Hospital had not been provided to the project manager.

The March 1999 public disclosure statistics for public hospitals have cited an overall percentage representation for Y2K readiness of 31%. This was in broad agreement with

audit findings in as much as it indicated that the majority of the project was still to be completed. It should be noted however, that this rating was an average for the three public hospitals and a break-down of the figures did reveal that significantly more progress had been made by the North West Regional Hospital and the Launceston General Hospital in the areas of technology and biomedical equipment and infrastructure. The overall percentage representation for Contingency Planning given was 26%, and this was also in broad agreement with audit findings.

The disclosure statistics indicated that the hospital project was on time and the target date for completion was 30 September 1999. Verification of the likelihood of attainment of these statements could not be produced by the hospital as a project schedule had not been developed.

An October 1998 survey response indicated that contingency plans for critical systems and processes had been completed, however, the response for the same question on the February 1999 survey indicated that the development of contingency plans was in progress and drafts would be completed by 30 April 1999. The February response was in agreement with the audit findings. Also, responses to the questions on testing for the October 1998 survey indicated that the agency had developed a comprehensive testing plan which addressed all systems. The February 1999 survey however, contradicted the earlier response by indicating that a comprehensive testing plan had not been developed and it was not in progress. Another response given in the same survey was also not in agreement with audit findings, as no formal test plans for any systems had been developed.

Comment from auditee:

'DHHS has contended that the discrepancies in responses to the Budget Committee surveys to a large extent reflect the poor survey design, which had insufficient instructions attached to ensure correct interpretation of the meaning of various questions, [and that as a result] *... the impression created was that the Agency was further advanced with the detail of its Y2K planning than in fact it was.'*

Timelines

All hospital departments had completed risk assessments but a project schedule showing the sequence in which remedial and contingency strategies were to be implemented had not been developed at the time of the audit. The timeline of 30 September 1999 had however been assigned for the completion of testing, remediation and contingency planning.

Information Gathering

The hospital had gathered information from a range of sources including the Internet (NSW Y2K Government Biomedical Database) and peers Launceston General Hospital (LGH), North West Regional Hospital (NWRH) and COSOPS. The Business Risk Manager facilitated information exchange between the three public hospitals as well as overseeing progress. Given that the NWRH and the LGH appeared to have made significant progress in a number of areas increased sharing of information may have been worthwhile. The Internal Audit section within DHHS had provided some quality assurance.

Awareness-Raising Activities

Awareness-raising activities across the hospital occurred primarily through completion of the business risk analyses. Staff of affected areas within the hospital including senior management had not met at the time of the audit, but it was intended that regular meetings would be held for the remainder of the year.

Conclusion

The Audit Office considered that the project could be capably managed by the Y2K Project Manager, the Hospital and Ambulance Service Division's Business Risk Manager and the Information Systems Manager.

Auditee Update

'Following the Audit of Royal Hobart Hospital undertaken in April 1999, substantial progress on Year 2000 Readiness has been made in all Tasmanian public hospitals. Milestones achieved include:

- *Compliance certification has been obtained for all building and environmental systems.*
- *Information provided by Telstra in response to the inventory of telecommunications equipment is currently being processed, and current indications are that there are very few items not Year 2000 compliant. Such items will be replaced.*
- *Compliance certification has also been obtained for critical biomedical equipment and other medical technology items. Remediation has been completed for all but a few items.*
- *Contingency plans have been completed for all functions of the public hospitals, and staff training and testing is in progress. This will largely be completed by 30 September, although on-going refinement will continue in the last three months of the year.*
- *Year 2000 patching of the major administrative information systems is on target and will be completed for all public hospitals by the end of August.*

The target date for Year 2000 Readiness is 30 September 1999, and this is expected to be achieved in most areas. However, there are some remediation subprojects which have experienced delays and will not be completed by this deadline. These include the replacement of the administrative support systems for the Emergency Medicine departments, Pharmacy departments and Pathology department at Launceston General Hospital. These schedules are reliant on vendor timeframes and will be completed in adequate time before the end of the year.

The Chief Executive Officer of the Royal Hobart Hospital who was appointed in April, has given the project strong support within the hospital and she personally reviews progress on a fortnightly basis. Risk Registers have been developed for all public hospitals, which are updated on a monthly basis to monitor progress of risk reduction. These are reviewed by both the Hospitals and Ambulance Executive Committee, and by the DHHS Y2K Steering Committee.

The public can be confident that the public hospitals will be fully prepared for the Year 2000. Tasmanian public hospitals have an excellent track record of being able to continue to provide services in the event of technology failures in the past, e.g. fires, blackouts, phone lines cut, IT systems down, equipment failing, and also in responding to community emergencies. While we do not consider that any of these specific failures are likely to occur on 1/1/2000, we can have confidence that such events will not reduce the quality of care given.'

TRAFFIC MANAGEMENT

The audit office carried out a review at the Traffic Management branch of the DIER during May 1999.

Testing

In December 1998 a departmental Y2K Task Force was established to coordinate the project across all divisions and branches. DIER's Project Business Plan contains details of project-based outputs that were the responsibility of the Project Manager. Amongst these were test plans that described the approach and activities to be undertaken in the testing of equipment that may have potential Y2K Problems, with the target date for completion being set at 31 July 1999.

Traffic Management Branch classified the traffic signals system as critical to its operations, a decision that was supported by the potential impact of Y2K Problems on public safety. A Resource Register was compiled to provide an overall picture of the equipment that supports this function. Further, a project plan was drawn up listing proposed actions plus targeted start and finish dates.

Tasmania's traffic signals system is comprised of three major components, the first of which is the Sydney Coordinated Area Traffic System (SCATS), a software program developed and supported by the Road Traffic Authority (RTA) of New South Wales and widely used throughout Australia. Its function is to centrally control and coordinate those traffic signals that do not operate in an isolated, stand-alone mode. SCATS operates in Hobart, Launceston and Burnie

Secondly, there are controllers that are responsible for the operation of traffic signals at individual sites and are either linked to SCATS or (in remote or less complex positions) operate independently in a stand-alone situation.

Finally, there is the Tasman Bridge gantry system in Hobart that controls the daily 'tidal' traffic flow system on the bridge. It encompasses the traffic signals, movable signage and master controller installed on the Tasman Bridge together with telecommunications equipment.

Extracts were generated from the traffic signal database to produce inventories of equipment employed throughout the state to enable the review of vulnerability of individual items within each of these systems. Traffic Management Branch's Y2K team based technical testing around a standard plan developed by British Telecom in 1997. Documentation in relation to test processes was to be generated from that process.

Testing was to be conducted as part of the contingency phase since upgrades or replacements would be required to first attain Y2K compliance according to information obtained.

IT Systems

Since SCATS has been developed and maintained by the RTA, information was sought from that Authority regarding Y2K compliance of its products as generic testing was being conducted in NSW. SCATS questionnaires were completed and returned to the RTA, which subsequently provided information as to the status of its range of software products. Some compliant items had already been obtained and orders have been placed for others.

The British Telecom tests were to be applied to the technical platform that supports SCATS and work was being done to inventory those items that would need to be included.

Information was also obtained from the supplier of the operating system regarding compliance of its products. To achieve compliance an upgrade was necessary and an order was placed for the necessary kits and operating licences.

In addition to the computers deployed to run SCATS, Traffic also had a backup mainframe. It had been used as a test platform and was successfully trialed with the date rolled forward from 2000 to 2010.

The only date-sensitive part of the Hobart's Tasman Bridge gantry system is a PC that functions as a master controller. Its BIOS and operating system were to be upgraded. Compliance information obtained indicated that an upgrade of the assembler software would be required and it was duly ordered.

Building and Environmental Systems

As controllers are located externally, the only critical building and environmental systems are the control rooms that house SCATS equipment in Hobart, Launceston and Burnie plus a control room at the Tasman Bridge.

The Hobart SCATS control room is housed in building that is relatively unsophisticated so far as building services are concerned. Existing services were to be assessed, however, and incorporated in the testing plan. Similar action was planned in respect of the Tasman Bridge control room. Launceston's SCATS equipment is located in a Police Service building and was included under the umbrella of the Police Service's Y2K activities. Burnie's SCATS equipment, too, was to be included in the testing plan.

Telecommunications Systems

Although telecommunications form an important link in some critical components of traffic signals, a critical rating was not applied. This assessment was justified by design features that allow networked controllers to continue safely functioning in the absence of central control (refer to the following section for more detail).

A variety of media are used to provide communications between SCATS and the controllers it coordinates together with ancillary communications circuits to camera equipment. This network mainly consists of DIER-owned cabling and is used for both SCATS and communications on the Tasman Bridge gantry system. Although little or no date dependent technology was used, telecommunications equipment that formed part of traffic signals systems would be included for testing of date functionality.

Some use had been made of Telstra products in the traffic signals system, namely private and dial up lines. The issue of Y2K vulnerability of Telstra products was being pursued at the Whole of Government level to which DIER was party.

Other Embedded Systems

Controllers, which can operate in either stand-alone or networked situations, monitor local traffic conditions and cause traffic signals to respond accordingly. They operate subject to certain pre-determined safety and efficiency parameters based on time intervals and/or traffic volume.

Safety considerations are a primary design feature of controllers, for example in networking situations controllers' operational thresholds cannot be over-ridden by the central computer. Also, there are fail-safe mechanisms to prevent dangerous events from occurring (eg conflicting green signals). Further, several levels of fallback are built in to counter problems of varying degrees of seriousness, that could ultimately lead to the automatic shutdown of a

controller. In this event traffic flow would be governed by the usual traffic laws and regulations.

Two different generations of controllers are used by Traffic Management Branch in common with other Australian authorities. The older type need a 'personality program', with a date burnt in, in order to function but this date is not used subsequently in processing activity. The manufacturer no longer supports these products so updating and testing of the date function was being done by Traffic's technical staff. For the newer devices software upgrades were available and some had already been acquired.

RTA had been performing generic testing on behalf its clients throughout Australia. Individual authorities still needed to do testing in their own environment, however, and DIER's Information Management Branch (IMB) was providing a test platform.

In-going and Out-going Supply Chain

Although some aspects of the in-going and out-going supply chain have already been covered, this issue was mainly being addressed at the Departmental level through the Whole of Government forum. Testing was to be covered under the contingency phase of the Y2K project and was anticipated to end on 30 September.

Compliance

Efforts had been made to establish the level of upgrading and replacement needed with respect to critical systems. Actions had been initiated to acquire the necessary items or expertise (with some already obtained). Compliance testing was to be undertaken subsequent to their receipt and installation.

End-to-end testing was done in a test environment with spare controllers connected to the backup mainframe computer. No major problems emerged as a result of this testing. The target date set for compliance by Traffic varied between 31 July 1999 for IT and embedded technology and 30 September 1999 for the remaining areas.

RTA was to make one of its officers available to assist Traffic with technical upgrading. Compliance verification was to be conducted after completion of the necessary upgrades with the target date of 31 July 1999. Given the small scale of remediation required for building and environmental systems the target date of 30 September 1999 appeared to be readily achievable. Compliance certification was to be obtained from telecommunications suppliers' web sites, while action in relation to Telstra products was being coordinated through the Whole of Government. The older type of controllers were to be tested after date changes were made. For the newer type supplier certification was to be obtained after in-house testing of recently acquired software upgrades. Traffic Management Branch had contacted its range of stakeholders with work in relation to testing the supply chain continuing.

Business Continuity

Under the umbrella of the Y2K Project Business Plan the Business Continuity Approach and a template for risk minimisation plans were developed concurrently.

Risk Assessment

Business risk assessments - based on expected consequences of possible failure - were completed last year providing a focus for testing and remediation activities. Risk

minimisation plans for IMB, assets controlled by Finance and Facilities Branch and Traffic Management Branch's draft plan were examined by the Audit Office.

Contingency Planning

At the time of the audit contingency planning by Traffic Management Branch was at an early stage, although a draft contingency plan had been produced within which the importance of inter-agency links with key service and emergency groups was stressed. Existing emergency plans and procedures (eg Tasman Bridge Emergency Traffic Plan) would provide the basis for development of Y2K-specific contingencies.

Criteria for Contingency Mode

Through responding to outages of the traffic signal system Traffic staff already have some experience of operating in a contingency mode. Traffic Management Branch intended to develop Y2K criteria for the full contingency plan. The process was under way with finalisation of the contingency plan targeted at 1 October 1999.

Staff Training

At the time of the audit no training had been conducted as contingency planning was in the early stages. As a further contingency measure extra personnel may bolster the number of key staff already designated for after-hours call out in the Emergency Procedures, for the period from late December 1999 to early January 2000.

Contingency Testing

The State Disaster Committee had requested Region Disaster Planning Groups to hold workshops for the purpose of assessing activities being undertaken by essential service providers. The project manager attended a workshop held in April and a further forum was scheduled for July at which time contingency issues were to be discussed.

Governance

Governance and reporting for Traffic Management Branch's Y2K project demonstrated an effective approach. Resourcing, whether in the form of funds or secondment of staff, had been made available to ensure that progress was made. The Audit Office formed the opinion that staff were comfortable with the direction and organisation of the project and believed that milestones would be achieved.

Project Sponsor

The project's sponsor was the General Manager Corporate Services who reported to the Deputy Secretary. Also, DIER had a Y2K Task Force with representatives drawn from each branch. Within each business unit there was a Y2K coordinator who worked closely with the project manager.

The project manager had prepared a departmental budget estimate for 1999-2000 and for Traffic Management Branch, funding of approximately $100 000 was identified for Y2K activities. This sum included the cost of one additional FTE for a period of two to three months to expedite the testing and remediation of controllers.

Reporting

There were regular lines of reporting on Y2K, with the project manager reporting to the sponsor each month and DIER business units reporting in turn to the project manager in a similar format. The task force, comprising the project manager and business unit coordinators, also meets monthly.

At the branch level, project status reports were generated monthly and provided details of a number of aspects including achievement on milestones, the work plan for the ensuing month, areas of concern, a progress summary and a financial summary. Information from these lower level reports was collated into a departmental report that also included a risk status summary for the areas of public safety and welfare, corporate applications and business unit issues.

DIER has participated in the monthly Public Disclosure Statistics process. The percentages submitted could not be supported by a rigorous, documented approach but, in line with the public reporting process, were based on estimated time and effort expended to date against that required to finalise a task. Statistics used by the Audit Office in this audit were those published for April 1999 and it appeared that the percentage figures in respect of readiness and contingency gave a satisfactory account of the state of Traffic's position at that time.

The target date of 1 October for readiness and contingency planning, which should allow adequate time for compliance testing to be undertaken, was likely to be met as schedules indicated that Traffic's Y2K project was proceeding satisfactorily.

Timelines

Milestones for completion and documentation of inventories and risk assessments had been achieved. The Traffic Management Branch project plan was developed with compliance and targeted end dates identified on the project schedule. Completion of testing was due on 30 July 1999 and it seemed likely that this would be met.

Information Gathering

Information had been gathered from a range of sources including the Internet (particularly the NSW government site), Standards Australia and the Australian Information Industry Association. Also, there was contact with peers in other states through the national body 'SMUG' – SCATS Management Users Group – which provided a forum for authorities to share information.

In December 1998 the project manager attended a conference on Y2K global management strategies in Melbourne from which a number of subsequent actions arose, such as project funding and whole of government issues with regard to communications.

Quality assurance had not been specifically sought for Traffic's Y2K project, although it was understood that RTA had applied quality management principles in its testing and remediation of SCATS on behalf of its clients. Similarly, some input on quality assurance issues was also available through SMUG.

Awareness-Raising Activities

Traffic had been diligent with regard to awareness-raising activities, which included staff bulletins with items on project news as well as specific-purpose messages from the project sponsor to all DIER employees.

Conclusion

At the time of the audit Traffic Management Branch's Y2K project appeared to have been adequately managed. Traffic should be in a sound position to manage incidents that may arise from the Problem, provided that the remaining testing, documentation and development of the contingency plan proceeds according to schedule.

HOBART REGIONAL WATER AUTHORITY

The Audit Office carried out a review of the Hobart Regional Water Authority during May 1999 at the Hobart Water premises.

Testing

The Authority had been conducting an audit of processes and systems that involved the documentation of item details, item analysis, threat, criticality and quality analysis. Definitions of criticality ratings categorised the higher risk items with the labels - 'Lives May Be at Risk' and 'Risk of Injury'. A detailed set of testing guidelines that outlined compliance criteria and a matrix of test processes versus component types had also been developed.

A Lotus Notes database was used to store the testing procedures and results for all inventoried items. The design of the database was such that access to compliance information could be readily gained. Project software had also been used to monitor progress and in order to facilitate the timely completion of testing and remediation processes outsourcing of these tasks was undertaken for several systems.

IT Systems

IT systems classified as having high criticality were the payroll, accounting, Electronic Funds Transfer (EFT) and telemetry systems. The human resource system, Payline, had been tested by the supplier and items had been identified, documented and prioritised for testing. Attache, the accounting software, had been registered as compliant with Standards Australia and the schedule indicated that testing and mitigation of the layered products for this system would be completed by June 1999. The EFT process had been inventoried but not tested at the time of the audit. Testing was to involve discussions with the bank to determine the compliance status of the systems used in this process.

Listing and testing of telemetry infrastructure was due to be completed by May 1999 and at the time of the audit the inventory was virtually completed and testing was well under way. Upgrades for mainframe infrastructure was expected to be completed by July 1999. The original version of the Supervisory Control and Data Acquisition (SCADA) system software was not compliant and modifications were to be made to the date functions by the contractor. Prior to performing these upgrades, a back-up of the operating system, application software and data was to be conducted.

The Authority sought the services of a computer firm in April 1999 to audit other IT infrastructure as well as to perform compliance checking and testing where possible. At the time of the audit, testing of all critical IT infrastructure had been completed and results revealed that there were some compliance problems with NT servers and three SCADA PCs running Windows 3.1. BIOS testing was also complete and all systems failing the rollover test were able to be successfully upgraded. Remediation of other non-compliant IT components was to be finalised by June 1999.

Building and Environmental Systems

Testing of all building services had been outsourced to consulting engineers. Results revealed that the fire indicator panel on the main Administration building was not time or date dependent and information on the compliance status of the fire pump system was still being sought. The security system software had been found to be not compliant and the air conditioning controls were still to be checked. It was intended that the remediation of non-compliant items in this category would be finalised by July 1999.

Supply of electricity to pumping stations is essential for water distribution to some locations and after examination of plans at the Tasmanian Electricity Supply Industry (TESI) Year 2000 Office, the Authority expressed confidence that the supply of electricity would not be interrupted. Nevertheless the Authority still intended to seek compliance information as well as to develop a contingency plan to mitigate against loss of power.

Telecommunications Systems

Testing and remediation of the radio telemetry system was to be undertaken by the contractor. Given that the network consisted primarily of devices without date functionality it was unlikely that Y2K problems would be encountered.

Network infrastructure consisted of hubs and layered network products. These items had been inventoried but were still to be tested as part of the outsourced IT infrastructure audit. Public Switched Telephone Network (PSTN) links were used to enable dial-up access to the SCADA system and statements on these links were still to be sought. TASINET maintains the PABX system and at the time of the audit the Project Manager was yet to obtain compliance information on this system from Networking Tasmania.

Other Embedded Systems

Municipalities reliant upon the supply of water from the Authority are the Hobart City, Glenorchy City, Derwent Valley, Clarence, Sorell, Kingborough, Southern Midlands and Brighton Councils. Reservoirs are supplied from a combination of catchment areas and water pumped from the Bryn Estyn station. During the summer period dependency upon pumped water is increased and previous data have revealed that at this time 70% of regional water needs originate from Bryn Estyn.

The Bryn Estyn pumping station and treatment plant is used to supply water to the majority of the regional reservoirs. It is to be thoroughly investigated for any Y2K problems as failure of this station can prevent the supply of water to Bridgewater, New Norfolk and other outlying Eastern Shore regions. The project schedule indicated that identification of components and risk assessment had predominantly been completed for this unit. The seeking of compliance information and testing of systems had, however, only recently begun and was due to be completed by June 1999. Remediation and mitigation of non-compliant items was to begin in mid-June and be completed by July 1999. A similar stage of progress had been achieved for other pumping houses with testing and remediation of critical components to be completed by August 1999.

The components responsible for controlling the reservoir levels and valves, namely, Remote Terminal Units (RTUs), Process Data Systems (PDSs) and Programmable Logic Controllers (PLCs) were also to be tested by the contractor. At the time of the audit it was indicated that RTU functionality complied with Y2K issues, but compliance was still to be determined for PDSs and PLCs. Firmware and software developed for each of these units was to be tested and mitigated by July 1999.

Chemical treatment of the water is managed by ratio controllers and as a field audit item compliance is to be determined by August 1999. Other critical field audit items to be tested by this date included the vigilant alarm dialler, the automatic timer for vigilant alarm and the chlorine leak detector. Other embedded systems including uninterruptable power supplies and vehicle electronic control systems were still to be inventoried at the time of the audit.

In-going and Out-going Supply Chain

The in-going and out-going supply chain was regarded as having the highest criticality because Y2K failure of a number of stakeholders could interrupt supply. Key beneficiaries and dependencies included the councils that managed reticulation from the Authority's reservoirs and the supplier of the turbidity meter which was used to measure water quality.

The Lotus Notes database had been used to categorise and collate customer and supplier compliance data. Initial letters seeking compliance information had been sent to all councils and meetings to discuss progress and project overlap had been planned. Risk assessments and testing of critical council items were also to be completed.

Compliance

The testing /compliance plan for the Authority was based upon the criteria provided by Standards Australia. These criteria were a minimum guideline only and, for critical or complex items, consideration was given to the application of more detailed testing. The Authority compliance certificate had provision for the transcription of testing and mitigation details as well as for the nomination of a compliance rating and confidence factor. These requirements ensured that the compliance status of items was unambiguously determined and recorded.

Compliance charts had been produced which showed percentage compliance for each category. The number of items which needed to be certified each month in order to attain full compliance by the target date of September had also been charted. These rates provided the manager with a metric for monthly performance.

An end-to-end test for IT, building and environmental, telecommunication and other embedded systems was not planned but system acceptance testing for upgrades and replacements was expected to occur through normal operation.

Business Continuity

The Millennium Bug Mitigation Project Plan defined objectives, stakeholders, scope, strategies and officers responsible for sign off. A project risk assessment of major tasks had been included and a breakdown described deliverables, deadlines and the estimated duration and effort for each task.

Risk Assessment

The Authority had devised a rigorous quantitative methodology of risk assessment. Processes and items were assigned a criticality in the form of a percentage and the product of these figures was used as the representative risk for each item. The degree of mitigation was also represented as a percentage - this was then subtracted from the unmitigated risk to determine a final percentage for mitigated risk. The use of clear definitions for risk classification facilitated the identification of critical systems and the prioritisation of remedial tasks.

Contingency Planning

Y2K-specific contingency planning was in a preliminary stage of development at the time of the audit with incident management procedures and a number of issues and preventative measures having been proposed. Identified risks requiring contingency planning included contamination of the water supply, loss of Bryn Estyn and other major pumping stations, loss of power, critical pipelines, the control system, communications, flooding and shortage of essential supplies.

Contamination of water could be realised through the plant failing to control the output of chemicals into the water or through upstream incidents at the Hamilton Sewerage Treatment Plant. Mitigation strategies included the placement of a second person for manual operation at Bryn Estyn, assessment of the Hamilton plant and the purchasing of monitoring equipment.

The Hobart City Council is dependent on the Authority for the bulk supply of water, but maintains some reticulation storage capacity (approximately one week) for short term disruption to supply. The hill top reservoirs at Ridgeway and Tolosa St will be filled prior to January 2000, ensuring a partial 'buffer' for the Clarence, Glenorchy and Ridgeway districts in the event of upstream problems or power failure. The Lake Fenton reservoir may act as an additional buffer provided the water quality is satisfactory. As stated previously though, some areas have no reticulation storage and therefore no buffer against failure of bulk supply.

Consideration was being given to the manning of all stations at the date rollover and manual switching of pumps was the proposed mitigation for loss of Bryn Estyn and/or other pumping stations. Also, the impact of decreased water quality as a result of failure of the chlorination process was to be managed through the issuing of 'Boil Water' alerts. Further, a repair crew were to be on standby to manage loss of any critical pipes due to power and water surges. Other proposed strategies included the use of a large number of manual operators for loss of the control system, radio communication in the event of loss of phone services, minimisation of reliance on Bryn Estyn in the event of flooding (caused by power failure and dam overflow) and stockpiling of chlorine and fuel.

The Authority was reviewing the existing Emergency Plan as part of the contingency process. This document addressed in detail the major risks faced by the Authority and the Standard Operating Procedures defined criteria for implementation.

Criteria for Contingency Mode

The Authority intended to develop criteria for the Y2K contingency plan as well as revising criteria listed in the existing Emergency Plan. These criteria would address a pre-defined number of system failures for a wide range of conditions. Given the degree of organisation and progress demonstrated to date it would not be unreasonable to expect that the milestone of 30 September 1999 would be achieved for this task.

Staff Training

Staff were not familiar with the existing plan at the time of the audit, however, presentations were to be conducted towards the end of the year to raise awareness and inform of roles and responsibilities. As a further measure, the Authority intended to ensure that operational, technical and field staff, were available for after-hours call out.

Contingency Testing

The existing plan had not been tested and documentation of incident management had not occurred. Walk-throughs were to be conducted to test the Y2K contingency plan.

Governance

Governance and reporting for this project appears to be of a high standard. All staff interviewed were comfortable with the direction and organisation of the project and confident that milestones would be achieved.

Project Sponsor

The General Manager of the Authority was the sponsor for the project. A business case had been produced that clearly outlined the project risk, a cost benefit summary and potential project benefits. While a separate Y2K budget had not been prepared, consideration had been given to levels of resourcing needed to ensure that project objectives were met. The cost benefit analysis estimated the total cost of external and internal resources as $180 000 and $214 000 respectively. It was intended that if any stages of the project required funding an application would be submitted to the project sponsor.

The Authority had ensured that specialised aspects of the project were managed effectively through the acquisition of expertise from external resources. Resourcing of the engineering and operational aspects of the project was therefore not an issue.

Reporting

The Y2K Project Manager had held meetings with the Manager of Corporate Services on a weekly basis since the inception of the project. Monthly written reports had also been produced for perusal by the project sponsor. These reports were thorough, clear and concise in their documentation of achievements and work pending. No major issues of concern were reported but provision was made for problems to be mentioned.

The Authority had been party to the monthly Public Disclosure Statistics process since May 1999. The project manager explained that readiness percentages submitted were determined by calculating the fraction of effort expended of effort required from the project schedule. As expected, the May figures showed slightly greater progress than that found by the Audit Office in April. For all categories, however, it seemed that appropriately adjusted percentages would be fundamentally accurate. Given the rigour which had been demonstrated to date in all aspects of the project it was likely that the readiness target date of 1 September 1999 would be met.

The contingency planning percentages were determined by estimating the fraction of effort expended of effort required rather than relying on the project schedule. For the majority of the services the estimates of percentages of planning completed was 33%, and since this component of the project had only recently commenced at the time of the audit this figure seemed reasonable. The target date of 1 October 1999 for completion of planning seemed to be achievable and the indication that the project was on schedule was in agreement with the timelines examined.

The Authority had not participated in the Budget Committee reporting process and therefore an assessment of this aspect of reporting was not undertaken by the Audit Office.

Timelines

Timelines for phases and tasks were determined using project management software. Progress towards the attainment of the major milestones (1 September 1999 for testing and remediation) and contingency planning (1 October 1999) appeared to be steady. The risk assessment for critical items had been completed and risk reduction was regularly monitored and updated.

Information Gathering

Information had been gathered from a range of sources including the Internet and other industries. In particular, a number of Y2K plans have been obtained from industry bodies and these had been used to develop the detailed testing guidelines. Contact with State Government agencies had also been a means of information gathering.

A quality checklist detailing deliverables, requirements, responsibility and acceptance sign off was included in the plan. Quality assurance had been sought internally through peer review of testing processes and strategies of mitigation. The outsourcing of components of the project to consultants and contractors with expertise also ensured that a high level of external quality assurance had been employed.

Awareness-Raising Activities

The Authority had been diligent with awareness-raising activities, which have encompassed presentations by the Project Manager and monthly staff bulletins. Meetings with operational staff were convened on a weekly basis and a number of meetings had been held with beneficiaries and dependencies.

Conclusion

A highly professional approach had been taken by the Authority in managing the Y2K project and the rigour demonstrated should see the Authority in a sound position to address any incidents that may arise from the problem, provided that the remaining testing and development of the contingency plan proceeds according to schedule.

Auditee Update

'Testing

Y2K Compliance Checking is on track for completion by 31 August 1999. Testing and Remediation for the Water Delivery is 96% complete as at 5th August 1999.

For Bryn Estyn Water Treatment Plant and Pumping Stations 99% of components had been checked and building services, telemetry and IT have reached 99%, 97% and 83% Testing and Remediation respectively.

The Program of checking Business Continuity has nearly completed with Suppliers, Field Audit Suppliers, Consultants and Payroll at 100%, 100%, 98% and 98% respectively.

IT Systems

The Payline system for Payroll for employees has now been certified to two levels as being Year 2000 Compliant. That is the Company performing the pay transfers has compliant software and the financial institutions receiving have compliant receiving software. The capability of the financial institutions to then deliver pay is a matter of public disclosures by those institutions and the information available at Tasmanian Government Fora on the Banking Systems is that it should be Business as Usual.

The SCADA and Telemetry system has been upgraded in August 1999 and is now certified as Year 2000 compliant.

A full end to end test of the SCADA and Radio Telemetry systems was completed successfully in a range of Dates from 31/12/1999 rolling over to 1/1/2000 and 28/2/2000 to 29/2/2000 to 1/3/2000.

IT Year 2000 Compliance has a few non-critical upgrades to complete and these will be integrated into an upgrade to the method of imaging the IT environment onto PC's in September 1999.

Building and Environmental Systems

The Security system software has been upgraded and will be tested by 1 October 1999. Further presentations by the TESI Year 2000 Office confirm a confidence in their Year 2000 program for Electricity.

Telecommunications Systems

Telstra statements on their items has indicated no problems and their program has been very thorough. An end to end test of the SCADA and Radio Telemetry systems was completed successfully and showed no problems in the Radio Telemetry systems.

TASINET has also issued a satisfactory Compliance Statement for the phone connections.

Other Embedded Systems

Examination of embedded systems was a major part of the Hobart Water Year 2000 program and was very thorough in identification. No compliance problems were found in any of the lower level instrumentation & electrical components. Most Compliance was sought using the Internet and a quality check of critical components by 2 engineers was used to sign off items with no date function.

Most items were found to have no date function to be tested.

Field Components' suppliers were judged Year 2000 Compliant from their Internet and written responses. Only 2 critical Field Components' suppliers were assessed for the Compliance of their internal Business Processes as it was judged that a failure in the Business Processes of most Field Component suppliers would allow the replacement of that supplier by another.

In-going and Out-going Supply Chain

Checking of the In-going and Out-going Supply Chain has proceeded satisfactorily and a total of 100 letters have been sent with a satisfactory response level, particularly in the critical supplier category.

The Program of checking Business Continuity has nearly completed with Suppliers, Field Audit Suppliers, Consultants and Payroll at 100%, 100%, 98% and 98% respectively.

Criteria for Contingency Mode

Contingency Planning has commenced in detail with the formation of a Team comprising Operations and Administration personnel. This team will be examining the identified contingency requirements and allocating them to specific persons for action if required. This will achieve a level of ownership of the Year 2000 Contingency by people throughout the organisation.'

STATE EMERGENCY SERVICE

The Audit Office carried out a review of the State Emergency Service (SES) during May 1999.

Testing

SES focussed on external and internal issues separately in managing the Y2K Problem. At the time of the audit greater effort had been directed towards managing external areas of concern through the facilitation of Y2K regional workshops. Outcomes of these workshops have been addressed in the section titled 'In-going and Out-going Supply Chain'. SES also planned to review existing generic state emergency plans to determine their suitability for a Y2K emergency and this is discussed in the section titled 'Business Continuity'.

The internal component of the project was in a preliminary stage of development at the time of the audit, with initial identification, risk assessment and mitigation of non-compliant SES systems and processes being conducted. Internal information technology, building, environmental and telecommunications systems were maintained by Tasmania Police and the testing for these systems had been addressed in the Audit Office's feedback report to Police. The number of remaining systems for which SES is responsible is low (a satellite phone, mobile base stations and vehicles) and therefore the development of formal testing plans was not considered to be necessary for these items. Testing would, however, need to be conducted and any required mitigation (remediation or contingency planning) was to be applied.

IT Systems

All IT systems used by SES were maintained by Tasmania Police and therefore the testing of these systems is described in the chapter on the progress of Police.

Building and Environmental Systems

The compliance of building and environmental systems at regional emergency coordination centres was also to be addressed by Police. The Southern and North-West regional centres rely upon back-up generators in the event of a power outage, however, the Northern branch does not have this facility. This was to be addressed through the installation of a new generator in this centre by 31 August 1999.

Telecommunications Systems

SES digital communications infrastructure was also maintained by Tasmania Police and testing of these systems had been accounted for in the Police assessment. The analogue VHF radio communications system used by the SES (identical to that used by Police) is shared by other Commonwealth, State and Local Government entities. The SES and the Department of Defence maintain a capacity for fixed and mobile intrastate HF radio communications. It also maintains an interstate HF radio communications capability from the Burnie centre. Each of these systems is comprised of analogue technology that has no date functionality and according to the Manager Operations compliance had been obtained from the supplier. Compliance checking for the satellite phone and the mobile base stations had been conducted, however, certification was not able to be located.

Other Embedded Systems

Apart from vehicle ignition systems the Tasmania Police project will address the testing of other embedded systems. It was the intention of the project team to determine the compliance status of vehicle ignition systems from Fleetcare.

In-going and Out-going Supply Chain

SES organised and chaired regional Y2K-specific workshops to facilitate the sharing of information between providers of essential services. Planning was not formally documented but a brochure did define the purpose and agenda of the sessions.

The report produced as a result of the workshops contained a synopsis of organisational preparedness, attachments of presentations and recommendations. The links forged between providers as a result of the highlighting of interdependencies was the major benefit to attendees. Also the increased networking capability assisted providers with the development of contingency plans.

SES also conducts approximately ten seminars annually on risk management and the development of emergency plans and procedures for governmental and non-governmental organisations.

Compliance

Tasmania Police was addressing compliance for the majority of systems. Test results for the systems for which SES was responsible, namely the satellite phone, mobile base stations and vehicles will be used to determine the most appropriate form of mitigation for these items.

Business Continuity

Continuity of business during and after an emergency relies upon the implementation of effective contingency plans. Generic plans jointly developed by SES and other government organisations, such as the Tasmanian Emergency Management Plan (TEMP) and Regional Emergency Management Plans (REMP), achieve this through prescribing procedures for the re-establishment and maintenance of essential infrastructure of a disaster-affected community.

SES did not consider these plans to be wholly adequate, however, for the management of emergencies arising from widespread technological failure. Therefore, a review was to be conducted with appropriate additions and amendments to be incorporated by September 1999. Also, to ensure functionality of plans at an operational level SES and the WY2k team planned to jointly develop a Tasmania Year 2000 Contingency Plan.

Risk Assessment

SES was to conduct a risk assessment of external parties to identify and prioritise areas of potential concern across essential service organisations. This assessment would provide a basis for the development of mitigation strategies for the Tasmania Year 2000 Contingency Plan.

Contingency Planning

The TEMP provides an overview of:

- The roles of organisations in emergency prevention, preparedness, response and recovery;
- The management structure for multi-organisational response and recovery; and
- The means by which states of alert, emergency or disaster are declared.

The response protocol is therefore key to emergency management. The current system is based on three elements – the lead combat authority, the control organisation and support organisations.

First the organisation with primary responsibility for a given type of emergency event is called the 'lead combat authority' and is responsible for dealing with the technical aspects of the emergency and for the command of its own resources. Secondly, 'control' is the overall management of emergency response in support of the lead combat authority and is normally vested in a senior officer of Tasmania Police. This may be required due to the necessarily restricted focus of the lead combat authority. Thirdly, 'support' organisations may provide specialist services in any given emergency event and the work of these agencies is managed by the controlling organisation.

Therefore, effectiveness of response depends upon the capacity of the lead combat authority, the controlling and support organisations to fulfil their obligations during an emergency. As this could in turn be dependent upon the effectiveness of Y2K projects of these organisations, assurance is needed in this respect before the capacity to respond can be confirmed. Consequently, SES was engaged in a review of state level and local government plans. Since the Tasmania Year 2000 Contingency Plan also relies on these plans review findings should be shared with the WY2K team.

After the TEMP the next level of reference in the event of declared and non-declared emergencies is the REMP. This plan outlines procedures for the coordination of government resources where the management of incidents exceeds the capacity of a council or statutory authority.

REMPs provide more specific terms of reference for the management of a state of alert, emergency or disaster than does the TEMP. Again however, successful implementation would depend upon the ability of the lead agency to cope with the emergency and respond effectively in accordance with the REMP. Thus there needs to be a high level of compatibility between the agency plans, REMPs and the Tasmania Year 2000 Contingency Plan.

In a declared event the REMP requires SES to establish a communications network to all affected organisations and provide regular situation reports to the Regional Disaster Controller (RDC). This presupposes that communications facilities are intact both within the lead agency as well as between the agency and SES, which needs to be the subject of an assessment either jointly or separately by SES and/or the Whole of Government Unit.

The existing TEMP and REMPs therefore do not address the full range of emergency scenarios which could arise in the event of wide spread technological failure (namely those arising due to power failure or loss of communications). They also presuppose that the response protocols and communications infrastructure of lead agencies will be operational. These issues should be addressed in the development of the Tasmania Year 2000 Contingency Plan.

SES contingency planning for internal processes and systems had just commenced at the time of the audit. It was intended that planning would encompass the deployment of all resources as well as the manning and back-up of power at emergency centres.

Criteria for Contingency Mode

Activation of the TEMP and the REMPs involves the notification of the RDC at Tasmania Police by the lead agency that a significant event situation exists. Then, if it is decided that a state of alert, emergency or disaster is warranted it may be declared by either the Director of Emergency Services, the responsible Minister or the Governor. The issuing of overall emergency management instructions to all agencies within a region then becomes the responsibility of the RDC. Administration of the TEMP and REMP at the operational level remains primarily the responsibility of agencies.

The ability of the lead agency to respond at the appropriate time therefore depends upon predetermined criteria for invocation of both the agency's emergency plan and criteria for establishing contact with the RDC. At the time of the audit SES were reviewing this aspect of state level and local government emergency plans.

The Project Team indicated that criteria defining activation of contingency mode for internal processes would be built into the SES Contingency Plan.

Staff Training

SES staff and volunteers undergo exercises three or four times a year to ensure familiarity with roles and responsibilities stipulated in plans. As part of the Y2K project, these same preparations were to be undertaken in respect of the SES Contingency Plan. It was intended that all centres would be manned and volunteers put on stand-by during the Y2K rollover. Further, SES had prepared a comprehensive emergency contact list for other agency officials at all levels of government. Amendments are made twice a year and for the Y2K date rollover a final review will be completed by November 1999.

Contingency Testing

All SES plans, including the TEMP and REMP, are tested through the exercising of scenarios and walk-throughs with a subsequent biannual review.

Governance

The requirement for a whole-of-government approach to be adopted in emergency planning for the Y2K Problem resulted in SES assuming a pivotal role in the organisation of regional workshops. Due to the small number of staff in the agency and the ease with which information could be exchanged verbally, formal documentation of internal management processes was lacking.

Project Sponsor

The project sponsor is the Director of Emergency Services. The Manager Operations stated that a separate budget had not been determined because it was assumed that existing resources would be sufficient and funding to date for the project had been adequate. The resources required to fulfil project goals, however, need to be determined so that tasks could be prioritised and any shortfalls addressed.

Reporting

The Y2K Project Manager had reported to the Corporate Management Group of the Department of Police and Public Safety in written form detailing activities of the Project Team. The Project Manager is also a member of the Whole of Government Steering Committee that met weekly.

Although the Project Team had produced reports on seminars, workshops and conferences, a regularised process of reporting had not been devised. In order to provide regular updates on the progress of the project, as well as to facilitate auditability, status reports could be prepared.

Since March 1999 SES has been party to the monthly Public Disclosure Statistics process. The Manager Operations explained that readiness and contingency percentages were determined by estimating the fraction of effort expended on internal operations and emergency management planning. The readiness percentage of 90% assigned to operations for April 1999 seemed rather high given that progress of SES internal systems was in a preliminary stage at the time of the audit. The nominated figure of 75% for effort expended on contingency planning also seemed to be high because planning for internal processes was only in the discussion stage in April 1999. Confirmation of the 60% figure assigned to readiness and contingency planning for emergency management planning was difficult to gauge. It would have required a detailed examination of the reviews conducted of state level and local government plans.

The SES did not participate in the Budget Committee reporting process and therefore the Audit Office has not undertaken an assessment of this aspect of reporting.

Timelines

Completion of risk assessment and testing was targeted for 30 September 1999. On the basis that risk assessment was a fundamental tool for further decision-making the Audit Office believed this date should be brought forward. Testing, remediation and contingency strategies could then be determined from knowledge of the associated likelihood and impact of risk of process or system failure.

Information Gathering

According to the Manager Operations information for management of the SES Y2K project had been obtained from a range of sources including Regional Y2K Emergency Management Seminars, WY2K Forums, Tasmania Police and the Emergency Management Association national conference. The only documentation provided to the Audit Office as evidence of the extent of this research was a report produced from the seminars.

Neither internal nor external quality assurance had been sought for the project and a form of peer review may have a number of systems in common.

Awareness-Raising Activities

Awareness of Y2K activities had been raised at SES through internal and external meetings, workshops, conferences and the web site.

Conclusion

SES had organised a number of Y2K workshops for essential service providers and this facilitated the sharing of information and methodologies. The Service should apply further resources and knowledge gained to the mitigation of internal processes and systems, as well as to the development of the Tasmania Year 2000 Contingency Plan.

TASMANIAN ELECTRICITY SUPPLY INDUSTRY

The Tasmanian Electricity Supply Industry (TESI) is comprised of three entities – the Hydro-Electric Corporation (Hydro), Transend Networks Pty Ltd (Transend) and Aurora Energy Pty Ltd (Aurora). The Hydro is responsible for generation, system control and hydro consultancy, Transend is responsible for transmission network service and Aurora is responsible for the distribution network service and electricity retailing.

TESI embarked upon a Y2K project in May 1997 and the current formal program was adopted in January 1998. The testing described in this section took place during May through June 1999.

Testing

Methodology

TESI had adopted a comprehensive Program Management Methodology that established the framework within which risk assessment, testing and remediation were being conducted.

The methodology involved four phases:

Dimensioning	is the identification of areas and degrees of exposure
Decision-making	is problem recognition, consideration of options and the achievement of a negotiated response by information owners
Actioning	is either unilateral...or bilateral...effort.... to rectify or mitigate a problem area
Proving	is the verification of the efficiency, effectiveness and satisfactory coexistence of any modification of a business process.

The project was divided into the following streams:

Enterprise	solutions spanning the business
Desktop	PCs
Verticals	company specific systems
Comms	telecommunications systems
Infra-structure	commercial and technical computing platforms
Embedded	hydrology, generation, buildings, protection and control, plant and equipment, distribution, vehicles
Contingency	develop and implement contingency provisions
External Relationships	external parties
Quality Assurance	test strategies, integration and end-to-end tests, audit of program activities.

TESI employed a specialised contractor to develop and implement a project plan for each stream of the project. All project plans (including schedules and details) were completed and functional by 30 September 1998.

Dimensioning and mapping of the problem for each stream made use of wall charts to represent commercial and operational processes.

Commercial Processes

Diagrammatic risk assessments for the commercial business processes used the following classifications:

Category	safety and welfare, security, revenue, external services, internal services and statutory and regulatory
Sensitivity	extreme, essential, used in business, documentation only
Severity	nature of the exposure
Mitigation	remedy, eliminate, work-around, tolerate
Remedial Priority	1st wave (completed by 31 December 1998), 2nd wave (completed by 30 June 1999), 3rd wave, 4th wave.

Processes were deemed to have 'extreme' or 'essential' sensitivity if interruption to business operation would occur upon malfunction of the process. It was preferred that non-compliant components utilised within these processes were either upgraded or replaced in the first wave.

Operational Processes

Diagrammatic risk assessments for the operational aspects of the business used the following classifications:

Sensitivity	high, medium, low, no clock/date dependency
Compliance Desktop	formal test, supplier certification, independent documented test, supplier documented test, independent compliance statement, supplier compliance statement
Mitigation	upgrade, replace/swap, tolerate with contingency, work around by de-activation of non-compliant interfaces, elimination.

The rating system used the term 'high' to categorise items for which failure would result in the interruption to supply of electricity. It was therefore synonymous with the terms 'extreme' and 'essential' which were used for commercial aspects of the business. Items falling into this category were required to undergo formal testing by TESI or supplier certification was to be provided, and non-compliant components were required to either be upgraded or replaced.

Processes and Systems

The Audit Office's examination focussed on critical systems and processes. TESI's initial risk assessment, however, only categorised processes according to business exposure. In order to review testing and mitigation activities it was necessary for the Audit Office to identify component systems that comprised processes. Critical processes could consist of a number

of systems that themselves may have a range of criticality ratings and it was therefore inefficient to consider all systems within a critical process. The Audit Office therefore sought information on criticality through discussions with employees who had specific knowledge of these systems.

Auditability and Mapping

Wall charts provided a visible audit trail of the business processes, their criticality and compliance status. The Audit Office could not, however, easily link processes and assessments on the wall charts to the databases, test processes, results and compliance certificates for several streams. An electronic system of cross-referencing (eg a master Hyper-Text Mark-up Launguage (HTML) document or relational database) that established links between critical processes, systems, databases, test process documents and certificates would therefore have aided auditability.

Quality Assurance

Quality Assurance (QA) for the program had involved the use of a quality plan to ensure that remedies were verified as acceptable for business operation. This had required the coordination of a wide range of testing methods, including the organisation of end-to-end testing and the continuing negotiation with major clients to ensure that inter-company interfaces remained operational.

Testing guidelines for technology components were based upon six standard criteria developed by the project team. These criteria were derived from the British Standard for Y2K compliance. The criteria related to date integrity, discrimination, process, order, calculation and leap year.

Detailed test processes for some streams were devised by the Project Management Office (PMO), but for others the processes were not prescriptive as a broad range of specialised technology needed testing. Where this was the case staff with relevant expertise had developed detailed scripts and testing processes. The rationale for this approach was based upon the argument that employees with intimate knowledge of the system were best suited to the development of detailed tests.

While quality plans had been built into the program methodology and did provide a level of assurance, the possibility remained that some tests may not have been adequately devised or implemented. At the time of the audit an informal system of quality checking was in place whereby the Project Managers could review field testing procedures, however, a regularised sign-off procedure at the testing process level (eg peer review) could prevent this from occurring.

Change Control

There is a risk that non-compliant items could be introduced inadvertently through routine acquisition, replacement programs or developed technology and prejudice systems that had otherwise been previously subject to testing and remediation. To counter this possibility a change control mechanism was instituted.

The process, well supported by a staff awareness campaign, required that a change control notification form be used to record the receipt of any such equipment and that a Y2K warranty be sought from the supplier or through the PMO. Audit was able to verify this system by following through an example in the embedded technology stream.

The distinct possibility remained however, that items (particularly intangibles such as software) could come into service and escape the change procedure. This control weakness

had been considered and various solutions instigated. Some areas within TESI submitted regular returns, including 'nil' returns, that were followed up in the PMO. For some other technical streams a central contact point was used to coordinate the supply of change control information.

IT Systems

Testing of IT systems had been addressed through the desktop, enterprise, infrastructure and vertical streams. Testing plans detailing the goals, objectives, exclusion, scope, constraints, related projects, organisation, deliverables, resourcing requirements and milestones had been developed for each stream.

Desktop Stream

The project commenced in July 1998 and the rollout of a compliant set of standard desktop products to 1600 PCs was completed by January 1999. An end-to-end test of the standard desktop was to be conducted by 30 June 1999 and the test plans and procedures were being developed. The quality plan for this stream required upgrades and vendor-supplied patches to be tested where applicable in accordance with the Change Control guidelines.

PCs which were used to access critical systems performed a critical function within the desktop stream and it was a requirement that they were operational at the Y2K rollover. BIOS testing had been conducted on all 1600 PCs in the first wave for this stream with results input to a database. At the time of the audit the database indicated that 3% of PCs failed the power-on/power-off rollover test and were to be retired or replaced. The 28% of PCs that failed only the Y2K rollover would have this date manually set at the appropriate time.

Testing of operation systems and applications was also conducted as part of the first wave of the desktop project. Upgrades of operating systems and applications were undertaken for most systems. Where this was not possible, follow up upgrades were to be conducted in the second wave. These were due to be completed before the end-to-end test was conducted in June 1999. Non-critical office-type applications (mail, calendaring, word processing) were also covered within the desktop stream.

Databases were developed to store test results on operating systems and applications. Information provided from these databases indicated that for the 161 Windows 95 machines, 86% were certified as compliant, 11% were not compliant (predominantly straight-forward matters to be followed up and addressed at a later date) and 3% were classified as 'other' (to be replaced or requested to leave until 2000). For the 1028 Windows NT machines, 94% were certified as compliant and 6% were not compliant or were classified as 'other'.

Desktop applications of significance were either upgraded to a compliant version or certified as compliant.

Enterprise Stream

The enterprise project had been well documented through a project charter and plan. The scope of work to be completed both for the project and for quality assurance and testing had also been documented in detail, as have procedures for in-house rectification.

The project plan had addressed testing and remediation of two critical systems. These are the Human Resource Management Information System (HRMIS or ACCORD) and the Materials Management Information System (MMIS or MATMAN). The two systems share data and are affiliated with a number of other non-critical associated applications.

The scope of the work for the project had been detailed in a compliance project document. Work statements and assignment briefs defining milestones, type of remediation to be undertaken (replacement, upgrade or rectification), work and task descriptions, deliverables and start and target dates had been included in this document. Impact statements defining the effort and cost of upgrading technology components had also been completed.

In order for the replacement of systems to be functional within the existing enterprise environment, rectifications had been made to interfaces and environmental systems by the project team and contractors. Final integration testing of these rectifications and replacements was to occur as a result of an integration test in August 1999.

Human Resource Management Information System (HRMIS)

HRMIS and associated applications (HRMIS Utilities, HR Warehouse), is a payroll processing package that was not compliant and due to be replaced by the Human Resource Information System (HRIS) at a cost of approximately $1m for each of the Aurora and Hydro companies. Originally, this replacement was to be completed by 31 March 1999 (based on a start in August 1998) but due to contractual difficulties it is now due to be completed by 31 October 1999. This will be done in two stages - the critical payroll features including will be installed by 31 July 1999 with the non-critical functions to be installed by 31 October 1999. The critical payroll features of HRIS were to be subject to the August integration test of enterprise systems.

An acceptance-testing plan for HRIS had been jointly developed by the project team in conjunction with the contractor and was being implemented by the supplier. The final end-to-end test was scheduled for August 1999.

Transend was to install another payroll service, Payline, in place of Accord. Installation was due to be completed by 1 July 1999. Transend indicated that certification had been received from the supplier for the Payline application.

Materials Management Information System (MMIS)

MMIS is the package that manages the critical systems responsible for job control, procurement, accounts payable and credit card payment. Installation and functional integration testing on the compliant operating applications uncovered many problems which were remediated by 16 May 1999, when verification was provided that the front end and production runs would continue to operate in the live environment. Y2K rollover testing of the system was to be conducted in August 1999 in accordance with the end-to-end test plan for enterprise systems.

Infrastructure

The infrastructure project entailed coordination of the achievement of compliance for the technical computing platform, the commercial computing platform and the communication network platform for each of the three companies. Enterprise, vertical and desktop applications therefore depended upon infrastructure covered by this project.

Hardware components to be tested as part of this project included data processing nodes, hardware controllers, network hubs, routers, modems and microwave equipment. Resident software to be tested included operating systems, database management systems, language compilers and other layered products.

Four main categories of infrastructure had been addressed. These were the Energy Control System (ECS), application servers, Virtual Memory System (VMS) and network file print servers and commercial communications infrastructure. The first wave of testing and

remediation addressed the energy control system and had been completed. The second wave of testing and remediation was addressing the other four categories and was due to be completed by 30 June 1999.

Compliance certificates had been completed for ECS, and application servers and the coded desktop stickers had been applied. For the VMS systems and the commercial communications infrastructure components information on upgrades was obtained from vendor web sites and at the time of the audit these fixes were being implemented.

Energy Control System

Although failure of this system would not cause immediate disruption to the continued supply of electricity it is integral to the effectiveness and stability of supply. The key feature of the system is that it provides a front end to operation through remote control and analysis of data provided by the Supervisory Control and Data Acquisition System (SCADA). It also performs the functions, of maintaining the frequency of supply and a stable line voltage in the event of loss of load. Following testing and modifications the application was rated as compliant in March 1999.

A risk analysis of ECS components of this network identified several high-risk items. These included the two energy control system servers and four control room servers. While the front end processor (FEP) for this system had not been included in this risk analysis, it had been identified by the ECS Systems Administrator as a critical system because it applied a date stamp to data passing from the RTU's to the ECS server.

Testing for the energy control and the control room server environments has involved the acquisition of compliance statements from suppliers. These tests revealed that the operating system - Digital Unix version 3.2 was not compliant, and subsequently it was replaced by the compliant version 4.0D. Compaq conducted an audit of the Digital Unix commands, scripts and utilities. Recommendations of this audit indicated that while testing processes were sound and should proceed as planned, a quality review was necessary to support test repeatability and the accurate extraction and analysis of data, as well as to support an accurate audit trail. Accordingly information on test processes was transferred to the Infrastructure and Quality Project Manager for review and this was conducted in December 1998.

Rollover testing of the FEP to the servers had not been possible because this was an embedded system. Testing had therefore involved the transfer of exception dates from the RTUs through the processor to the Alpha server. Since these dates were successfully transferred and no significant problems emerged from the supply chain end-to-end test of this system the processor has been rated as compliant.

The ECS was also included in the supply chain end-to-end test that was conducted in April 1999. The procedures and results of this test are detailed in the section 'Compliance'.

Application Servers

The application server component of the project addressed NT systems (hardware and software) used to support server applications. NT servers underwent BIOS testing and service pack 4 was applied to attain full compliance. While the project schedule indicated that all server systems would be upgraded to this level of compliance, only the system that supports the critical application, HRIS, has been addressed in this report.

It was intended that HRIS would operate in an NT environment on two Compaq 7000 servers. Documentation indicated that Service Pack 4 had been successfully installed on

both production servers and confirmation had been received from Compaq that these servers were compliant.

Transend indicated that certification for the IBM system upon which Payline resides was expected to be received from the supplier.

Virtual Memory Systems

The VMS stream within the project had addressed Alpha work stations, Virtual Address eXtension (VAX) mini computers/servers and the operating systems residing on these machines. Mainframe testing was based on the acquisition of compliance statements for machines and operating systems, since BIOS testing was not possible with these systems. Testing for mainframes had also relied upon the development of a dedicated test facility known as Y2Knet. Information Technology Services and Solutions (ITSS) pilot upgrades were also conducted in the first wave as a preliminary exercise. The project schedule indicates that these upgrades were successfully conducted on a VAX and a DEC Alpha system.

MMIS and the customer interface system Frontline both operate on Alpha servers over VMS. Confirmation of compliance had been received from the supplier of these systems. The same upgrades to VMS were being implemented for the Frontline system and it was expected that these were to be completed before the end of the second wave.

Network File and Print Servers

The network file and print servers are used to manage the storage and printing of documents within Local Area Network (LAN). There are a total of 46 print servers that had been identified in the inventory to undergo testing and remediation and of these 30 had been completed. From the total of 46 only two servers had been designated as posing a high risk to the business and one of these had been fixed.

Commercial Communications Infrastructure

Commercial communications systems reviewed in the infrastructure stream had included routers, hubs, bridges, concentrators, terminal adaptors and communication servers. For the most part switching devices within this network did not utilise date features and for this reason they were not considered to be critical to operation. This was verified by the successful supply chain end-to-end test for which all non-compliant switching devices did not present any problems.

Commercial communication servers that had been flagged as significant included the VAXs which concentrated the output from other mainframes so that it could be monitored from other terminals as well as the host for the firewall. According to the project schedule these systems had not been addressed as yet.

It was planned that finalisation of the infrastructure project would involve a post-implementation review of certificates and documentation on compliance as well as the issuing of disposal certificates.

Vertical Stream

Vertical stream project and quality plans have been developed for each of the three companies. A significant number of systems have been classified as having extreme or essential sensitivity within this stream, however, discussions with the Project Manager have revealed that the actual number of critical systems was much less. A risk assessment that

more rigorously reflected the importance of a system in an overall business context would have facilitated the audit of this stream.

Five important systems examined by the Audit Office were Frontline – the customer information database, Infinity – the treasury accounting system, Plato – used for valuing portfolios, Fintracs- used for the transfer of funds and Troublecall – used to log faults reported by the public. The testing of these systems had been postponed to the second wave due to on-going development as well as the considerable time required to develop testing processes.

Frontline

The Frontline system is the principal computer application used by Aurora for the management of day to day relations with customers, including all the financial transactions and as such it is integral to the management of revenue. Inputs for the system are received from Service Tasmania, Australia Post, Commonwealth Bank and the metering systems. The original system and releases have been developed in-house in a Forte 30G2 contemporary environment. According to the Infrastructure Services Team Leader this version of Forte has been certified compliant.

The application was to be tested primarily through the end-to-end test with remediation occurring for non-compliant problems after they have been identified through this test. The component of Frontline that manages the output to service connections had, however, been tested through the use of scripts to identify date-related code. Results of tests were positive, however, the end-to-end test was required to confirm the compliance of this component of the system.

The end-to-end test plan had recently been completed and it was to be conducted as soon as the dedicated testing facility using representative commercial computing equipment was reconfigured.

Infinity

Infinity is the Treasury Accounting System used for the management of loans, swaps, forward agreements, and foreign exchange. As testing could not be conducted in a live environment, alternative means of verification were being investigated. As a second wave item it was intended that remediation of this system would be completed by 30 June 1999.

Plato

Plato is the performance system used to value portfolios based upon loan data from Infinity and it is used to manage interest rate risk. The Treasury Risk Officer had been conducting testing on this system and to date no Y2K problems had been identified. Nevertheless, as a contingency the team formed to work with this system was to develop spreadsheets which would perform the functions of this program.

Fintracs

Fintracs is a finance system utilised by TESI for the automatic transfer of funds on a daily basis. While the Treasury Risk Officer explained that there were a number of work-arounds which can be adopted in the event of failure of this system the wall charts indicated that the system was essential for accounting and settlement.

The supplier had indicated that a statement of compliance would not be issued, instead the project team could make use of the supplier test facility to determine whether a suitable level of compliance had been achieved. Partial testing had been conducted on the facility

using mock cheques and to date no problems had been found. Most major Australian financial institutions had also been conducting testing on Fintracs and problems had been resolved as they came to light. For this reason, it was not expected that the system would present a significant problem with the Y2K rollover.

TroubleCall

The TroubleCall software was not compliant and according to the vertical stream database a rewrite of the code was to be completed and installed by 14 July 1999. The Interactive Voice Response system upon which TroubleCall resides was also not compliant and according to the database the supplier should have installed the required patch and equipment.

Building and Environmental Systems

Building and environmental systems were reviewed as a part of the over-all issue of embedded technology, all of which was coordinated by the Project Manager. Individual 'Buildings Embedded Technology' work sheets, covering component identification, were used to compile an inventory of building services from which a database was compiled. Not all TESI buildings were included, however, as power stations were considered to be part of the generation assets that they house rather than buildings *per se*.

For those building services that did appear on the database, details were shown for equipment and fittings that could conceivably be vulnerable to Y2K problems, encompassing access control, air conditioning, fire alarms, lifts and uninterruptable power supplies. Commensurate with the level of risk, various compliance measures were sought, ranging from compliance testing by TESI at the highest risk through to a supplier compliance statement at the lowest.

Tests, supported by documentation detailing test criteria, had been issued for the 12 high-risk items, that is those requiring TESI compliance testing or supplier certification. The testing status of individual items was recorded in the database and in four cases tests of high-risk items had been completed.

Most tests with respect to buildings had been completed and the results were available. Software upgrades had been sought from the supplier of a non-compliant system. It was anticipated that re-scheduled testing would be completed by the end of June.

Telecommunications

Much of the primary supply chain, that part of the system that actually generates and distributes electricity, comprises relatively simple electro-mechanical equipment not prone to Y2K risks. The secondary supply chain, which overlies the primary, is responsible for providing monitoring and supervisory functions and as such relies heavily on communications. The Energy Control Centre's (ECC) role is to monitor certain areas of the electrical grid. Information about the status of circuit breakers and current and voltage transformer measurements from sub-stations, power plants, etc., are processed and transmitted via RTUs to the ECC. Based on this information more or less power can be brought on line or circuit breakers can be remotely operated to ensure the required system configuration. All of these actions are carried out through the medium of the telecommunications system.

If communications were to be lost or disrupted due to Y2K problems there would be no immediate effect on output from the system, provided that no other incidents occurred simultaneously. During this time, however, another emergency, such as substantial shedding of load through a major customer going off-line, would be difficult to respond to. It is this

potential combination of problem scenarios that has actually occurred in some overseas networks that could trigger cascading effects and in turn could lead to the system state becoming critical.

The importance of telecommunications was recognised and various levels of back-up protection added as a way of minimising the possibility of losing these facilities. In addition to the safeguards engineered within individual communications systems there is a multi-level approach that confers a further degree of security by having a number of different, independently operating systems. The first level is TESI's own digital microwave radio system, second is the leased trunk mobile radio system and third are Telstra products with some satellite phones also in service.

An inventory of telecommunications equipment was taken and the details were then loaded into a database. Following compilation of the database, risk assessments were made by Systems Services and high-risk items identified. Due to the importance of telecommunications in monitoring and managing the network, as well as its pivotal role in voice and data communications a high level of risk was assigned to much of the networks. Not all high-risk items are subject to date sensitivity, thus the number scheduled for remediation in the first wave was reduced. Compliance verification information was sought and obtained directly from telecommunications suppliers or from their Internet sites.

As part of the overall planning process for the end-to-end test on the West Coast concluded in April, a telecommunications project plan was developed to cover relevant infrastructure. The digital microwave radio system, which is TESI's principal communications network, was extensively tested during this exercise.

The Audit Office noted that the telecommunications consultant was lost to the project before completion of his tasks. This had caused some delays in documenting progress made to date.

Digital Microwave Radio

The digital microwave radio network is owned by TESI and exists independently of Telstra's network. It is used for the full range of normal business communications – voice and data – as well as controlling the supply of electricity via the secondary supply chain through the ECC.

Much of the high-risk componentry (both hardware and software) utilised in the digital microwave network had been sourced from one company. Compliance statements were obtained indicating what versions of software were compliant and those that needed upgrading. PMO procedures stipulated that testing should be undertaken, even after upgrading, because of the level of risk assigned to this plant. This was one of the objectives of the previously mentioned end-to-end test.

Test results were examined by Audit and it was found that the only problem that came to light was corrected by means of a software patch after which the system operated without fault.

As a result of the end-to-end test the Y2K preparedness of the digital microwave radio system seemed to be satisfactory. Software upgrades, in line with suppliers' recommendations, were continuing although the versions currently deployed presented no practical problems during the test.

Trunk Mobile Radio

The service provider of the trunk mobile radio network had guaranteed service levels with respect to Y2K readiness.

TESI provides bearers to some of its more remote sites that would not otherwise be covered by the service provider. Access units used with this system are not date-sensitive. Trunk mobile radios were used during the end-to-end test but were not tested themselves.

Telstra Products

Use of the publicly owned Telstra network by TESI is limited due to the organisation's strategic decision to develop its own digital microwave radio system and the trunk mobile network. Nevertheless, TESI does use some Telstra products such as ISDN, tie lines and leased data lines to supplement its own communications facilities.

The use of ISDN is limited to ECC monitoring and supervisory functions in four locations that are not served by the organisation's own networks. Due to the previous reliable performance of ISDN and the small, discrete areas involved these links were not rated as high risk.

Satellite Mobile Phones

The role of satellite mobiles is very limited and is mainly restricted to use as a telemetry system for hydrological data logging, although they could provide a back up to other forms of voice communications. This lack of date sensitivity, combined with their limited deployment, resulted in them being viewed as non-critical.

Other Embedded Technology

The Program Management Methodology referred to earlier was supported by a number of more detailed plans at a lower level that were developed specifically for embedded technology.

The electricity supply chain is a complex system in which embedded technology has come to play an increasingly large part. Six separate elements were identified, namely hydrology, generation, protection and control, distribution, plant and equipment, and motor vehicles.

Hydrology

This category covered equipment used for purely hydrological purposes and other items that log data and provide the front end of telemetry systems. There were 71 items in this sub-division: 10 were classed as high risk and 61 as low. The majority of low risk items were associated with water flow measurements and their potential failure was regarded as an acceptable risk that would only result in a limited reduction of water management efficiency.

Most high-risk items were transmission line tension meters. These devices that are fitted to a minority of transmission lines and measure the tension on a line and gauge its state of operation: excessive current can lead to annealing of the conductors which may ultimately cause damage or even failure of the line.

The status of individual items requiring compliance testing or supplier certification had been recorded and in the case of the high-risk items tests had been completed. The tension meters were non-compliant (since they do not use 4 digit year formats) and as a result they were entered onto a Non-Compliance Register. Details of their non-compliance had been forwarded to the appropriate Risk Manager for advice on the remedial action to be taken.

Generation

The generation section of the electricity supply chain covers all embedded technology components in power stations, including building fittings such as intruder and fire alarms.

Engineering staff of the Hydro's Consulting Business Unit (CBU) visited each power station, head works, canal gate, pumping station etc. to record all items of plant. A large proportion (85%) was found to have no date sensitivity but 340 remained. Risk assessments yielded the following results; 47 low risk items, 113 medium and 180 high.

Supporting documentation was obtained from suppliers regardless of risk category. Low risk items were checked against supplier certification statements, medium risk items were type-tested on a sample basis, while each high-risk item was individually tested on site.

At the time of the audit the status of high-risk items was as follows: 110 found to be compliant, 46 non-compliant and 24 still in progress. A Non-Compliance Register was maintained for all such items, whether high, medium or low risk.

There were a number of different types of equipment at a variety of locations in the high-risk category. The largest groups were the very early smoke detector used in tandem with other alarms to protect generators, man-machine interfaces and an assortment of other devices such as trash racks, intake gate controls and generator governor oil-level monitors.

The most common reason for non-compliance in the high-risk group was related to problems of 2-digit year storage capacity. Nevertheless the devices in question would continue to function since the date was not used internally within the equipment or communicated to other devices.

An exception to the above concerned station sequencing computers on King and Flinders Islands. These devices are used to determine the operating order of diesel generators on each island. They are non-compliant and were to be replaced before the end of August 1999.

Protection and Control

This segment of the electricity grid is largely the province of Transend and it encompasses equipment installed in both the primary and secondary supply chains. The former consists of generators, transformers, circuit breakers, isolators and transmission lines while the latter comprises those devices (meters, communications, etc.) installed to enhance management of the network by the ECC. Generators have their own protective equipment, which is treated in this part of the report.

The function of the protection and control equipment is to protect major items of plant in the generation and transmission grid, such as sub-station transformers, from excessive voltage or current in the event of faults. Generally, the grid has been designed to high standards of reliability so that there is more than one level of protection.

An up to date inventory of protection and control equipment yielded 1 770 items that were then entered into a database. From this starting point, electro-mechanical equipment with no date functionality was culled, reducing the number of items subject to review by 927. Against an overall rationale of system stability the remaining 843 items were categorised as follows; low risk 237, medium 318 and high 288. At the time of the audit the status of high-risk items was as follows: 106 found to be compliant, 109 non-compliant and 73 still in progress. A Non-Compliance Register was maintained for all such items, whether high, medium or low risk.

There are two main types of high-risk non-compliant equipment. Firstly, there are relays and teleprotection devices in substations that may communicate with similar plant in other locations. Their purpose is to detect irregular voltage and current states on transmission lines and they time and date stamp trip and alarm events. In case of faults they provide an extra level of protection should local stand-alone protection equipment fail. Their non-

compliance is related to a 2-digit format for date display, which may be remediated through a later software version.

The second class of non-compliant protection and control equipment is the RTU. RTUs are used for sensing and reporting real time states of the network and also for the control of various other activities initiated from the ECC, such as opening or closing valves or dam gates. They time stamp events and provide a detailed sequence of actions reflecting network performance. These devices, too, have a 2-digit year capability that may not be crucial in terms of their operation but makes them non-compliant in terms of the PMO's approach.

Audit was advised that there are three devices at radially supplied Transend substations. Their testing would require significant switching of the distribution system and/or some short periods of outage to avoid longer periods of outage to consumers during the tests. As the probability of a Y2K problem has been assessed as very low, testing is considered inappropriate in these cases.

Distribution

In the main, the distribution arm of the electricity supply chain belongs to Aurora and includes ground and pole mounted transformers, regulators, reclosers and RTUs.

Distribution equipment had been assessed with regard to the likelihood of date sensitivity. Three categories were applied: likely, unlikely or none. Aurora's distribution network is almost exclusively composed of unintelligent electrical, pneumatic, hydraulic and electro-mechanical components completely lacking date functionality. The outcome of this process was that of an original total of 25 039 items almost all – 24 950 (transformers and feeders) were culled. The remaining 89 items (RTUs and reclosers) were categorised as follows; low risk 3, medium nil and high 86. A Non-Compliance Register was maintained for all such items irrespective of risk rating.

The function of reclosers is to detect various types of sub-optimal performance on a line and open the circuit if certain predetermined limits are exceeded. It then recloses the circuit if appropriate criteria are met. Reclosers also have the capacity to log data and record the operational conditions on a line. In these situations RTUs are used in conjunction with telecommunications systems to allow system controllers to access the data logged by reclosers.

Supporting documentation was obtained from suppliers regardless of risk category. Low-risk items were checked against supplier certification statements or test procedures, medium-risk items were type-tested on a sample basis, while high-risk items were originally intended to be individually tested on site. However, due to similarities between the individual items a sampling approach was subsequently employed. Testing showed that all were non-compliant due to a date format that displayed a 2-digit year; functionality was not impaired. A software upgrade was planned by 31 October 1999.

Plant and Equipment

This category contained a total of 576 items and was a catch-all covering both office machines - such as faxes, photocopiers, video cassette recorders (VCRs)– and technical test equipment used either in workshops or the field. Approximately a third (169) had been culled since they had no date functionality whatsoever. All remaining items had been assessed as low risk since their failure to operate would not prejudice the supply of electricity.

Motor Vehicles

At the time of the audit TESI's combined fleet strength comprised 1 133 units (including trailers, mechanical aids, motor cars and commercial vehicles). A risk assessment of 'low' was assigned to the fleet. Statements of compliance had been either from the Internet or directly from the respective suppliers.

In-going and Out-going Supply Chain

The external relationships stream had addressed compliance of the in-going and out-going supply chain for TESI. This stream focused on the development of registers for dependencies (supply goods and services) and beneficiaries (accept services provided). Readiness evaluations were being conducted on high-risk dependencies and the project schedule indicated that the evaluations for high-risk beneficiaries would be completed by July 1999.

The readiness evaluations for dependencies had involved the compilation of a report on areas assessed and corresponding company responses. Ratings of compliance for each area were also included. Hard copies of compliance statements obtained from a range of sources (eg letters, web sites) had been filed for the purpose of readiness evaluation.

Upon completion of the readiness evaluations it was intended that company business exposure profiles would be formed and then appropriate actions implemented. The project schedule indicated that this would be completed by August 1999.

ECS was developing contingency plans to deal with the event of extreme supply voltage fluctuations that could arise in the event of the loss of a major customer load. These plans would also involve joint contingency plans which had been developed by the project office in conjunction with the major customers. On the basis of commercial confidentiality, joint contingency plans were not made available to the Audit Office. The Project Manager stated, nonetheless, that all large concerns had been addressed and major customers were making appropriate efforts for Y2K readiness.

Compliance

End-to-end testing can be regarded as the ultimate confirmation of compliance. Within TESI's Y2K program an end-to-end test was defined as 'the verification of satisfactory working of an element or multiple elements of business operation, usually including external parties'. During the period 12–19 April 1999 such a test of the electricity supply chain was carried out; it involved the following:

- generation, transmission and distribution of electricity to customers in north west Tasmania;
- micro-wave voice and data communications from the west coast to Hobart - over the longest telecommunications path;
- full-blown centralised control of relevant system segments at a back-up site;
- forward dating of the test components and rolling over to sensitive dates in the time slot September 1999 to January 2001; and
- integration with normal operation of the remainder of the electricity supply chain.

The test covered six west coast power stations with a combined output capacity of 620MW out of a system total of 2509MW (25%).

A formal project was conducted to plan, prepare and execute the test. Prior to testing all components had passed compliance verification, incorporating stand-alone and integration tests. Procedures for the test were documented, reviewed and practised in advance of testing.

As a result of testing there were no supply outages or interruptions and the system was stable during the test. Only two minor problems were found that could be attributable to Y2K issues.

The success of this major testing program provided assurance of operational integrity for the electricity supply chain as well as the ECS and the communications networks.

IT Systems

End-to-end test plans had been developed for desktop, supply chain (ECS and communications) and financial systems (Frontline, MMIS and HRIS). These plans specified the scope, anticipated constraints and timing of the end-to-end tests. Test scenarios had been described in the plans and forms have been developed which allowed for completion of details on results, analysis and resolution on these scenarios.

Desktop

Remediation was completed for all desktop products, apart from the 'follow ups' of software which were still to be addressed. An end-to-end test was to be conducted in June 1999 of all desktop environments.

Enterprise

Rectifications to interfaces and environmental systems had been made for HRIS and MMIS. Installation of the new HRIS was still to be conducted upon completion of testing by the supplier. An integration test of all enterprise systems (apart from the low risk features of HRIS) was due to be conducted in August 1999. This test had yet to be developed.

Infrastructure

Remediation of all critical ECS infrastructure had been completed. This infrastructure had also been subject to the 'supply chain' end-to-end test.

Test findings were that no uncontrolled failures in the electricity supply chain occurred, the electricity system was particularly stable during the test and no customers experienced noticeable perturbations. These findings therefore indicated that remediation of the ECS had been successful.

Vertical Stream

Anomalies that arise as a result of the end-to-end test of the Frontline application were to be addressed on completion of the test. According to the QA project schedule, end-to-end testing was to be conducted on the system from 16 June 1999 to 2 July 1999. Scenarios were to test the receipting, reading, service request, street light, statement, debt collection and general ledger components of the system.

Building and Environmental Systems

The majority of testing of building and environmental systems had been completed and compliance verification was continuing. Testing for the upgraded software for the main Hydro and Aurora access control system was to be completed by the end of June 1999.

Embedded Technology

An end-to-end test of the electricity supply chain was carried out April 1999. The test involved a scaled down version of the entire system from generation to distribution but also included communications, ECS and backup facilities across a range of rolled forward dates. Procedures were documented, reviewed and practised in advance of testing.

Compliance verification had been achieved for individual components before the test. As a result of testing some minor remediation had been needed and this was completed.

Hydrology

All verification actions in this stream had been completed. The project manager has received advice on non-compliant items from the appropriate Risk Manager. Respective remedial actions were to be addressed in the third wave.

Generation

Testing in this stream was substantially complete with compliance verification continuing on the basis of test results. The necessary upgrading of the non-compliant sequencing computers on the Bass Strait islands was scheduled for August 1999 with compliance verification to follow.

Protection and Control

A small number of test reports remained outstanding and were scheduled for completion before the end of June. The Contingency Arming Scheme had been disabled and remedial actions in other areas of protection and control were on-going.

Distribution

Testing of distribution plant had been completed but not all test results had been received in the PMO. Compliance verification was anticipated by the end of June 1999.

Plant and Equipment

Since the items that comprised this field were rated as low-risk compliance verification had been rolled in to the third wave.

Motor Vehicles

There were almost no Y2K implications with regard to motor vehicles and thus no remedial actions were planned.

Telecommunications

The West Coast end-to-end test demonstrated a high state of Y2K capability in the digital microwave radio network. Compliance verification had been completed although some further testing may be scheduled later in the year.

Compliance certification had been provided for trunk mobile radio. Compliance verification with respect to Telstra products, in light of their limited application within TESI, appeared to be satisfactory.

In-going and Out-going Supply Chain

It was intended that a review of actions and updating of profiles would be conducted until the end of the year for the external relationships stream.

Business Continuity

External relationships had been considered and various business units within each entity had categorised their stakeholders according to the level of criticality of the relationship. Good communications had been maintained with stakeholders through a range of actions, including site visits to the PMO where briefings and tours were conducted.

Risk Assessment

Risk assessment had been conducted upon business processes across TESI. This approach had enhanced management of the Y2K Problem as a business risk issue. It also ensured that all elements of business processes were addressed in the risk assessment. The assessment process involved the distribution of the survey forms to all Business Process Owners (BPOs). Operative staff then charted the processes and assessments in the PMO, with BPOs later examining these and confirming or modifying the assessment. As a third step general managers were asked to conduct 'sanity checks' to corroborate the ratings.

Performing risk assessments on processes has allowed the PMO to identify systems associated with processes for the purpose of subsequent testing and mitigation. It has not, however, facilitated the prioritisation of systems in terms of criticality as not all systems are necessarily of equal importance in a given business process. Ranking of systems individually within streams or processes is not seen as necessary by Project Managers since the PMO intend to test and mitigate all systems. Auditing of tested and mitigated systems, though, in an organisation of TESI's size and complexity requires critical systems to be identified.

Contingency Planning

Five areas were identified in respect of contingency provisions – the preliminary stage of contingency development. These were the supply chain, people welfare, strategic for business, business processes and joint contingency provisions. Separate master plans that contained details of scope and objective, methodology, timetables and milestones had been developed to expand the provisions for each of the TESI entities. The strategic directives outlined in the master plans provided a framework for more concrete plans and actions. A range of potential scenarios were covered such as unavailability of major plant, interruptions to operations or loss of communications, etc. The provisions then specified individual actions that should be taken and the target date for implementation. Provisions in the 'general' category remained the responsibility of the PMO while the others (namely electricity supply chain, conduct of business, joint arrangements and people welfare) rested with TESI staff.

Within the TESI business units some work remained to be done to complete the various actions stipulated by the master plans. In some areas, where restoration of service or response to unforeseen events was part of the usual mode of operation, this would not necessitate a large amount of work. In these locations existing emergency or action plans exist already (as at the ECC), while in others a greater degree of effort would be necessary as emergency situations are less commonly encountered.

Some examples of initiatives taken as part of this process were the stockpiling of critical spares, revocation of holiday leave for key personnel or the early production of cheques from the accounts payable system to more evenly spread workloads and minimise risks at the crucial dates.

The Hydro had participated in the Lifelines project coordinated by the SES and supported by Emergency Management Australia. This involvement necessitated on-going activities to identify and reduce risks to essential services (lifelines) including the review and enhancement of existing emergency management plans and procedures. To support this role SES recommended that the Hydro liaise with other lifeline agencies to predict interdependency implications of power failures.

IT Contingency Provisions

The Computer Disaster Management Plan, developed by an external firm of data security consultants was a comprehensive document. Responsibilities and procedures to be followed by nominated 'action persons' were clearly described with checklists and procedures supported by detailed schematic drawings and charts of the IT network deployed at every site in the state. Testing and updating of the plan was part of the on-going maintenance agreement with the consultants. Theoretical, desktop tests had been conducted, however, live tests had not due to the significant disturbance that would be caused to normal operations. Criteria for invoking the plan were not specified, although it is understood that this would be the subject of the next programmed meeting with the plan's authors.

Accounts Payable Provisions

A number of work-arounds had been developed to address potential failure of MMIS and were detailed in the Master Plan. These included the review and development of procedures of manual operations of the general ledger, changes to allow direct entry of job costing data, budgeting, EFT payments, stamp duty payments and cheque processing in the Y2K context.

Some work had already been done in relation to a variety of finance and accounting operations that would support those actions listed in the Master Plan. As an example, Audit obtained copies of business process contingency provisions, previously developed by staff at Aurora that aimed at providing guidelines for continued operations in a manual mode.

Billing Provisions

Actions specified in the Master Plan for billing were aimed at providing additional redundancy for the Frontline system. Some examples were assessing the practicality of hard copy manual operations and work-arounds, determining the criticality of third parties for Frontline and developing alternative means of receiving debtor files for external agency payments.

HR Contingency Provisions

The Audit Office examined a draft version of a disaster recovery plan for the HRIS project that would be used by Hydro and Aurora. This plan contained much pertinent information including configuration of the system, spare facilities available for emergency use, an analysis of risks with proposed mitigation through to procedures associated with follow up assessment of the plan after normal operations were resumed.

Supply Chain Contingency Provisions

Both Hydro and Transend identified the electricity supply chain as requiring the greatest attributable effort for contingency planning and Master Plans for each of these companies have been completed. Examples of actions specified within this area for the Hydro encompass testing of all machines that are capable of 'black starting', planning for the situation of loss of power to the ECC or dealing with the loss of reactive load from a major

customer. For Transend examples of actions specified are appropriate manning for protection and control equipment and the determination of high-risk embedded technology equipment that can be isolated during Y2K-sensitive periods.

The Audit Office reviewed a copy of the manual that dealt with transmission line emergency restoration. It appeared to have been written in 1995 and although it showed signs of later updating, it did not reflect the new structure of TESI since the disaggregation of the former HEC. As a result, many parts seemed to be out of date including details of contact personnel.

ECS Contingency Planning

The System Control Manager had recently produced a draft Y2K contingency plan. A number of elements were defined within the plan, including periods identified as requiring manning provisions, major contingency events (ECS failure, backup control system failure, communications failure) and disposition of the disaster management group. Manning of the power system was the key strategy for the contingency plan and on-call availability of staff for nominated key locations was identified as a priority.

The draft plan provides an overarching approach that is to be adopted in the event of failure of the above-named systems. The Manager Systems Control intends to include additional detailed material.

Criteria for Contingency Mode

Some disaster recovery plans and emergency procedures do not specify criteria for invoking, revoking and functioning in a changed mode of operation. This will be addressed under contingency plans, the majority of which are still to be refined.

Staff Training

Training of staff in contingency mode was not regarded as a high priority since the emphasis in contingency provisions had not been on developing new plans or procedures but on strengthening those that already exist and which are familiar to staff. As well, staff were encouraged to more actively identify risks and take steps to reduce them. In addition, some TESI staff regularly gain experience of operating in a contingency mode, since their work required them to respond to power outages caused by unanticipated incidents or equipment faults.

Contingency Testing

The approach to contingency testing, as indicated in the Master Plan, required that BPOs identify Y2K vulnerabilities and decide whether testing is necessary or not. The level and type of contingency testing to be undertaken was viewed by the PMO as being the responsibility of BPOs.

As with staff training mentioned above, a degree of testing and review of emergency response procedures already occurred through day to day operation of the electricity supply chain because of the need to respond to unforeseen incidents.

Governance

Program Structure

The Program Director had overall responsibility for the coordination of the TESI Y2K capability program across the three companies. The Program was overseen by the steering committee, comprised of the Program Director and the three Chief Executive Officers (CEOs). It met monthly (with minutes held by the Program Director) and a variety of reports regularly tabled. Additionally, the steering committee visited the Program Management Office (PMO) to be briefed on particular aspects of the program's progress and to have the opportunity to question the project managers at first hand. Each TESI company had its own Y2K Executive Management Team (EMT) which held monthly minuted meetings. Aurora and Hydro had dedicated Issues Management Teams (IMTs) whose aim was to ensure that previously identified Y2K risks were being addressed as well as tackling particular problems in their respective Y2K projects.

Monthly Y2K update reports were received by the Board of each company. Within each company the Business Entity Risk Managers (BERMs) were responsible for the business entity Y2K budgets. This involved the forecasting of expenditures by financial year/quarter for defined areas, the determination of options for individual expense items and the provision of warnings for cost overruns.

BPOs were responsible for compliance of major processes within each company for Y2K purposes. BPO dealings were principally handled via work statements that were negotiated, supplied and agreed prior to commencement of any program client activity. These were subsequently used as the acceptance sign-off medium. The administration of contracts with internal and external service providers was handled by BERMs. Key decisions were made by business stakeholders, BERMs and BPOs. Major internal service providers included the CBU and ITSS.

Program Management

The TESI project had adopted management guidelines set out in 'Project Management/Program Consulting Guidelines'. The guidelines required the development of quality plans for each program consulting area, the maintenance of a project diary by each project manager and the escalation to the Program Manager of any exceptions that could not be resolved immediately. The guidelines defined decision-making limits for project managers including acceptance procedures for external compliance certificates.

The PMO acts as a central coordinating body for the achievement of Y2K capability. Consistency in the format of documentation was ensured through the use of standard templates for diaries, plans, progress reports, assignment briefs and work statements.

Role of Sponsors

The CEOs for each company are sponsors for the project. Each month sponsors are provided with trend graphs of compliance verification, a road map of the status of the project, change control information and collated progress reports. Project managers for the enterprise, quality and contingency streams have met with all the CEOs at least once to discuss progress and identify pressing issues at an executive level.

Reports received by CEOs in relation to Y2K activities originated from a number of sources, amongst which were EMT, IMT, both the Program Director and Manager, Internal and external audit and Project Managers. This diversity of sources ensured that a range of views was provided with respect to progress.

Budget

Table 1 details budgetary and expenditure information for the three companies in respect of Y2K.

	1998-1999		1999-2000	
	PMO $m	Other $m	PMO $m	Other $m
Aurora	0.39	0.21 – remediation 0.32 – replace E-mail system 1.00 – replace HR system	0.24	0.42 – remediation & contingency provisions
Hydro	0.60	0.83 – HRIS system replacement 0.90 – audits, remediation, contingency provisions 0.29 – replace E-mail system	0.61	0.36 – ITSS 0.30 – recoveries 0.18 - contingency 0.16 – generation
Transend	0.09	0.05 – audit & test supply chain & buildings	0.06	0.04 – contingency deployment 0.10 – contingency materials & supply chain rectification

Table 1: TESI Y2K Expenditure

Transend's actual operating expenditure for 1998-1999 was considerably less than the budget because significant over-estimates had made for the replacement of protection, control and building equipment.

Adequate resources appear to have been allocated to the project as evidenced by the fact that expenditure was under budget in some cases. Also, staff expressed confidence that sufficient funding would be available to ensure the project's success.

Reporting

Progress Reports

Progress reports are produced weekly by project managers and these are made available to the Program Manager through the network. The collated reports, together with an issues register, are then provided to the Program Director.

Budget Committee Report

TESI completed the survey that was distributed in May of 1998 for the Quarterly Budget Committee reporting process. There were no major discrepancies between the explicit

responses that were given and audit findings, however, for several questions responses were not given in the format required.

Public Disclosure Statistics

TESI is providing Public Disclosure Statistics on a monthly basis. According to the Program Manager the percentages representing Y2K Readiness and Contingency Planning were determined, firstly by providing a weighting of attributable overall effort to areas and secondly, by providing estimates of percentage completed in each area. These estimates were determined based upon a judgement of the fraction of hours expended of the total hours required within an area.

The four key services which are addressed in these reports are the connection and supply of electricity, accounts payable, billing and payroll. Each of the companies has provided percentage-readiness figures, where appropriate, for the process areas associated with each of these services. Processes which utilise the critical systems addressed in this report appear to have been weighted appropriately.

Published readiness percentages and readiness target dates were broadly consistent with the Audit Office's assessment. The weightings used to determine the contingency percentages however, did appear to be inappropriate and could have caused inaccuracies in the final figures.

Timelines

Risk assessments for business processes were completed in May 1998 and for supply chain they were completed in February 1999. Project schedules that address management and testing for first and second waves had been developed using project software. This enabled program staff to estimate the resources needed for each task as well as to monitor progress of the project.

Although Project Managers intended to complete testing of critical systems before 31 December 1998 (milestone for first wave completion) there have been a number carried over to the second wave. These included some vertical systems and the replacement of the HR system that was due to be completed in the third wave.

A chart detailing percentage completion for program milestones produced by TESI showed that certification of the technical platform and the standard desktop rollout was complete. Second wave enterprise solutions were depicted as almost complete, however, this did not seem to take account of the new HR system for which compliance has not been confirmed.

Certification of the commercial platform and attainment of compliance for second wave vertical systems were approximately 20% behind target according to the chart. This had occurred because of the need to conduct testing out of office hours on some systems. Also, problems in acquiring test facilities for Frontline had caused delays in the vertical stream.

The remediation of embedded technology appeared to have made least progress relative to other streams, however, this was in line with expectations and the stream had fallen only slightly behind schedule. This may not be a significant concern given the small number of items actually requiring remediation.

Year 2000 Capability Road Maps were prepared for company CEOs. The maps included a reference to the HRIS component but apparently only to the interface rather than the system itself which was shown to be complete in June. Replacement of HRIS was being treated as a separate project with a later completion date and this aspect was taken into account in the preparation of the Public Disclosure Statistics.

Research

Assistance and information with respect to the Y2K capability program had been sought from a range of internal and external sources including ITSS, CBU, Internal Audit, the Whole of Government forum, audit firms, Electricity Supply Association of Australia (ESAA) and the North American Electric Reliability Council. ITSS provided system information as well as services to the project group and the CBU consists of engineers who usually operate as a commercial consulting arm of the Hydro, but who were involved in developing and refining embedded technology databases. Internal Audit units provided quality assurance and in the case of the Hydro furnished risk reports to management. TESI has participated in the Whole of Government forums since the program's inception early in 1999. This forum has provided the opportunity for exchange of ideas and information. ESAA provides a forum for the sharing of Y2K information across electricity authorities and companies. Its role is one of facilitation rather than regulation and TESI has tabled progress reports as a part of this process. This contact has enabled TESI to keep abreast of developments and to share its own insights with other providers.

A number of external audits had so far been commissioned from consulting or accounting firms some of which were made available to the Audit Office. The project team adopted some of the recommendations made in these reports, but not all. A report from November 1998 found that urgent attention was required where significant weaknesses exposed the business legally or operationally or detracted from internal control systems. Issues identified included: the ability of the project to meet the Wave 1 milestone, the definition of the Wave 1 milestone, management of individual project task slippage, implementation of the new HRIS system and analysis of the first impact date of critical systems.

More recently, a consulting firm reviewed the embedded technology stream in May 1999 with two issues identified for further action. Firstly, it was reported that notification regarding change control processes did not appear to be informing the project team in a timely manner. Secondly, a lack of detail was cited in some procedures that require decision making, the audit trail of decision-making, and the transfer of information between Project Members.

The management response in respect of change control agreed with that finding. Tighter procedures based on the existing procedures and forms and information provided on the business entity Intranets were instituted to alleviate this situation.

The Audit Office found that the audit trail for embedded technology items was reasonable, however, the communications, infrastructure, enterprise and vertical streams were not as auditable. In the case of embedded technology links between test sheets with accompanying results, databases and wall charts were easily verifiable and cross-referenced. For the other streams test sheets and results were not always available within the PMO and the connections between databases and sources of test information were not readily mapped.

Awareness Raising Activities

Awareness activities had been diligently undertaken since the inception of the project. Coverage had focussed on all internal and external stakeholders with extensive campaigns to promote PMO activities.

Internally, awareness had been raised via the assignment to BPOs of the implementation of testing, remediation and contingency planning. Meetings are regularly held to discuss issues as they arise. Discussions with project managers also revealed that impromptu meetings were held with field staff on a needs basis. The Intranet site, 'Insite', had been established to facilitate awareness of the Y2K capability program across the TESI companies.

Through the external relationship stream, various awareness-raising strategies had been employed. Joint contingency provisions were being developed with major customers and regular tours were conducted of the PMO for external stakeholders. Newsletters and posters had been circulated and articles reporting progress had appeared in local newspapers. The Program Manager had also conducted presentations to Whole of Government meetings to update the governmental sector regarding TESI's Y2K progress.

Conclusion

The program methodology had fostered a conscientious attitude and approach to the management of the Y2K problem within the PMO. This was especially exemplified by the efficient organisation of the embedded technology stream (widely seen as the greatest area of vulnerability within the electricity supply chain) which had been handled in a methodical, thorough and capable manner. Management of other streams had also demonstrated similar high standards. The incorporation of quality assurance, through dedicated resources in the PMO and audit (internal and external) had provided valuable feedback for refinement of the program.

The Audit Office was of the opinion that enhancements in auditability could be achieved through improved documentation in the areas of risk assessment, mapping and testing.

The Audit Office concludes that TESI appears to be well placed to manage incidents that may arise from the Y2K problem, provided that the remaining testing and development of the contingency plan proceeds according to schedule.

BIBLIOGRAPHY

Australian Bureau of Statistics. 1998. *Year 2000 Problem*, Cat. no. 8152.0, ABS, Canberra.

Australian National Audit Office. December 1998. *Getting Over the Line – Selected Commonwealth Bodies' Management of the Year 2000 Problem,* AGPS, Canberra.

_____. Questionnaire. 'Performance Audit of Commonwealth Agencies' Preparedness for the Year 2000 Problem.' 1997.

Atex Media Solutions. 1999. 'White Paper: The Year 2000 Problem and Year 2000 Compliance.' http://www.atex.com/y2k/whitepaper/problems.htm (2 February 1999).

Australian Broadcasting Corporation. 'Govt Promises Funds to Battle Y2K Bug'. http://www.abc.net.au/news/state/tas/mettas-16mar1999-1.htm (16 March 1999).

Australian Personal Computer. 1999. 'Y2K: A Regional Snapshot'. http://apcmag.com (1 February 1999).

_____. 1998. 'Y2K: The Desktop Disaster Plan'. http://apcmag.com (28 January 1999).

Barrett, P. Auditor-General, ANAO. 'Audit – The Best Management Tool in Year 2000 Resolution.' Address to the Canberra conference:' Surviving the Year 2000 Computer Crisis', 21 August 1997.

Bridel, H. 1999. 'Biomedical Testing Notes'. http://www.y2k.gov.au/biomed/html/tetsting.html (5 February 1999).

Charter. 1998 Charter Supplement: *The Year of Living Dangerously: Preparing for the Millennium Bug,* (November 1998).

Computer Connections. 'Year 2000 Embedded Systems'. http://speakeasy.org/~loren/Year2000/embed.htm (16 February 1999).

CTI Datacom Inc. 'Y2K Network Services Overview.' 1998. http://www.ctidata.com/y2k (2 February 1999).

Department of Communications, Information Technology and the Arts. 'Government Increases Level of Y2K Disclosure' http://www.dcita.gov.au/nsapi-text/ (3 March 1999).

_____. 'Y2K Disclosure Legislation Passes Senate' http://www.dcita.gov.au/nsapi-text/ (3 March 1999).

Department of Premier and Cabinet. 'Whole of Government Year 2000 Project 14 Business Plan', 14 April 1999.

_____. 'Year 2000 Public Report', March to July 1999.

Department of Treasury and Finance. 'Risk Management – Discussion Paper' May 1997.

Gartner Group. 8 January 1997. 'An Introduction to Business Continuity Planning'.

Information Strategy Unit, Department of Premier and Cabinet. Internal Document. 1998. 'Year 2000 Strategic Plan - Draft', 16 January.

_____. 1999. http://www.dpac.tas.gov.au/branches/isu (4 February 1999).

_____. 1998. 'Quarterly Budget Committee Year 2000 Reporting Framework.'

_____. 21 May 1998. 'Year 2000 Readiness Quarterly Report.'

Jabbour, L. 1999. 'Time Is Running Out!' http://www.standards.com.au/tas/1998/feb/features. (5 February 1999).

Kyrou, E, Partner - Mallesons Stephen Jaques. *Australian Company Secretary.* 'Y2K Implications for Directors' Indemnities.' February 1999.

Management Advisory Board and its Management Improvement Advisory Committee. 1996 '*Guidelines for Managing Risk in the Australian Public Service.*', AGPS, Canberra.

NSW Year 2000 Home. 'Year 2000 Contingency Planning.' http://www.y2k.gov.au/html/contingency.html (1 February 1999).

Office for Government Online. 'Year 2000 Contingency Planning Guidelines- Version 2.' December 1998.

_____. Questionnaire: 'Year 2000 Project Phases.'

_____. 'Year 2000 Project Office', (5 March 1999).

_____. 'Year 2000 Quarterly Reporting Framework', (2 July 1998).

_____. 'Year 2000 Testing Strategies-Version 1.2', (July 1998).

O'Neill, M. KPMG Seminar. 'Y2K – A Potential Liquidity Crisis', March 1999.

Standards Australia. 'AS/NZS 4360:1995 Risk Management' 5 November 1995.

_____ 'The Application of the Australian/New Zealand Standard AS/NZS 4360 – Risk Management within the Corporate Structure.' http://www.standards.com.au/tas/ (29 January 1999).

State Emergency Service. 'Emergency Management Initiatives'. http://www.soutcom.com.au/~tasesn/inits.htm (8 March 1999).

_____. 'Tasmanian Essential Services' (8 March 1999).

Tasmanian Audit Office. Special Report No 25, March 1998.*The Year 2000 - Are We Ready?*

Tasmania Year 2000 Information Disclosure Bill 1999.

Tasmanian Electricity Supply Industry. 'Year 2000 Capability Statement'. http://www.hydro.com.au/year2000/compliance.htm (17 February 1999).

Tasmania, House of Assembly, Pages 1-38. *Debates,* 29 April 1998 Part1 Pages 1-38 http://www.parliament.tas.gov.au/.

Tasmania, House of Assembly Estimates Committee, 16 November 1998, http://www.parliament.tas.gov.au/.

Tasmania, House of Assembly Estimates Committee, 18 November 1998, http://www.parliament.tas.gov.au/.

Telstra Press Releases. http://www.telstra.com.au/press/ (17 February 1999).

The Year 2000 Support Centre. 'Looking for Automated Equipment/Embedded Systems in your Organization'. http://www.support2000.com/embsyst.htm (17 February 1999).

Treasury Board of Canada Secretariat. 'The Year 2000 Challenge: Federal Government Monthly Progress Report', 16 February 1999.

United States General Accounting Office. *Year 2000 Computing Crisis: A Testing Guide*. November 1998.

Year 2000 Compliance Definition. http://www.info2000.gc.ca/definitions/ComplianceDef_E.htm (2 March 1999).

Y2K Register: Tools, Services, Products. http://www.y2kregister.com.au (5 February 1999).

_____. MP77-A Definition of Y2K Compliance http://www.y2kregister.com.au/define.html (5 February 1999).

Y2K-Status.Org.,'Telecommunications Problems'. http://www.y2k-status.org/TelcomProblems.htm (17 February 1999).

RECENT REPORTS

1992	SPECIAL REPORT NO. 1	REGIONAL HEALTH SUPPORT SERVICES
1992	SPECIAL REPORT NO. 2	STUDENT TRANSPORT
1993	SPECIAL REPORT NO. 3	EDUCATION INSTITUTIONS CLEANING SERVICES
1993	SPECIAL REPORT NO. 4	STANDARD OF ANNUAL REPORTING BY GOVERNMENT DEPARTMENTS
1993	SPECIAL REPORT NO. 5	MUNICIPAL SOLID WASTE MANAGEMENT
1994	SPECIAL REPORT NO. 6	ADMINISTRATION AND ACCOUNTABILITY OF GRANTS
1994	SPECIAL REPORT NO. 7	REGIONAL HEALTH MEDICAL REVIEW
1994	SPECIAL REPORT NO. 8	WASTEWATER MANAGEMENT IN LOCAL GOVERNMENT
1995	SPECIAL REPORT NO. 9	HERITAGE COLLECTION MANAGEMENT
1995	SPECIAL REPORT NO. 10	OFFICE ACCOMMODATION MANAGEMENT
1995	SPECIAL REPORT NO. 11	RECORDING AND REPORTING BY GOVERNMENT DEPARTMENTS OF THEIR NON-CURRENT PHYSICAL ASSETS
1995	SPECIAL REPORT NO. 12	TENDERED WORKS
1996	SPECIAL REPORT NO. 13	NURSING COSTS IN TASMANIA
1996	SPECIAL REPORT NO. 14	REVIEW OF PERFORMANCE INDICATORS IN GOVERNMENT DEPARTMENTS
1996	SPECIAL REPORT NO. 15	CASH MANAGEMENT IN LOCAL GOVERNMENT
1996	SPECIAL REPORT NO. 16	DEPARTMENTAL ACCOUNTING MANUALS AND COMPLIANCE WITH PROCEDURES
1997	SPECIAL REPORT NO. 17	AIR TRAVEL
1997	SPECIAL REPORT NO. 18	REVIEW OF LAND INFORMATION
1997	SPECIAL REPORT NO. 19	COMPLIANCE WITH SUPERANNUATION GUARANTEE ARRANGEMENTS
1997	SPECIAL REPORT NO. 20	REVIEW OF COMPUTER CONTROLS IN GOVERNMENT DEPARTMENTS
1997	SPECIAL REPORT NO. 21	SPECIAL INVESTIGATION INTO ADMINISTRATIVE PROCESSES ASSOCIATED WITH PRESERVATION AND MAINTENANCE OF THE PORT ARTHUR HISTORIC SITE
1997	SPECIAL REPORT NO. 22	LAND INFORMATION AND ADVERSE POSSESSION
1997	SPECIAL REPORT NO. 23	MANAGING SCHOOL MAINTENANCE AND MINOR WORKS
1997	SPECIAL REPORT NO. 24	FURTHER REVIEW OF PERFORMANCE INDICATORS IN GOVERNMENT DEPARTMENTS
1998	SPECIAL REPORT NO. 25	THE YEAR 2000 - ARE WE READY?
1998	SPECIAL REPORT NO. 26	CAPITALISATION AND REPORTING OF ROAD ASSETS IN TASMANIA
1998	SPECIAL REPORT NO. 27	USE OF MOTOR VEHICLES IN GOVERNMENT AGENCIES
1998	SPECIAL REPORT NO. 28	PAYMENT OF ACCOUNTS IN GOVERNMENT AGENCIES
1999	SPECIAL REPORT NO. 29	COMPETITIVE TENDERING AND CONTRACTING BY GOVERNMENT DEPARTMENTS