a stitch in time

facing the challenge of the year 2000 date change
The Audit Commission promotes the best use of public money by ensuring the proper stewardship of public finances and by helping those responsible for public services to achieve economy, efficiency and effectiveness.

The Commission was established in 1983 to appoint and regulate the external auditors of local authorities in England and Wales. In 1990 its role was extended to include the NHS. Today its remit covers more than 13,000 bodies which between them spend nearly £100 billion of public money annually. The Commission operates independently and derives most of its income from the fees charged to audited bodies.

Auditors are appointed from District Audit and private accountancy firms to monitor public expenditure. Auditors were first appointed in the 1840s to inspect the accounts of authorities administering the Poor Law. Audits ensured that safeguards were in place against fraud and corruption and that local rates were being used for the purposes intended. These founding principles remain as relevant today as they were 150 years ago.

Public funds need to be used wisely as well as in accordance with the law, so today's auditors have to assess expenditure not just for probity and regularity, but also for value for money. The Commission's value-for-money studies examine public services objectively, often from the users' perspective. Its findings and recommendations are communicated through a wide range of publications and events.

For more information on the work of the Commission, please contact: Andrew Foster, Controller, The Audit Commission, 1 Vincent Square, London SW1P 2PN, Tel: 0171 828 1212 Website: www.audit-commission.gov.uk
Summary

The year 2000 poses problems for all organisations that use computers and equipment which is dependent upon embedded systems.* The problems stem from the way in which dates are stored and used. They could occur before, on or after the turn of the millennium.

For the NHS and local government there are serious risks to life and health:

- hospitals could be susceptible to a malfunction of medical equipment;
- social workers may be prevented from accessing the child protection register;
- patient systems may refuse to allow the booking of appointments for the year 2000 or beyond;
- traffic lights may stop working, increasing the risk of accidents;
- communications systems used by the emergency services might fail to work, increasing risks to the public; and
- regular payments to those in need could be disrupted if benefits systems are unable to assess correct entitlement.

Authorities and trusts are also part of a complex web of business relationships where failure in one area can have significant knock-on effects elsewhere. For example, a failure in a supplier’s systems could lead to a shortage of critical medical supplies.

Preparation for the year 2000 is therefore a major management challenge. Chief executives are responsible for ensuring that their organisations are ready. Those organisations that have delayed taking action run an increased risk that key services will fail. Organisations or managers may be legally liable for any injuries or losses caused by failures of systems.

The Audit Commission has written this paper to help members, non-executive directors and chief officers in local government and the NHS to minimise the risk of serious disruption to the delivery of services resulting from a date-related failure in a critical system.

Throughout 1997/98 staff from District Audit, the Commission’s in-house provider of external audit services, have been assessing year 2000 preparations by authorities and trusts. This management paper is based upon the results of those reviews undertaken in the six months to March 1998. It provides a mid-term report on the progress made by authorities and trusts and identifies the action required in the next 18 months and beyond.

It contains the following key messages:

- services may be at risk because local authority and NHS year 2000 projects are, generally, behind schedule;
- progress in resolving problems associated with embedded systems is slower than for computer hardware and software;

* A general purpose definition of ‘embedded systems’ is that they are devices used to control, monitor or assist the operation of equipment, machinery or plant. ‘Embedded’ reflects the fact that they are an integral part of the system. All embedded systems are, or include, computers. The simplest devices consist of a single microprocessor (often called a “chip”). Institution of Electrical Engineers; Technical Guidelines 9, Embedded Systems and the Year 2000 Problem, 1997.

For the NHS and local government there are serious risks to life and health
• the cost of remedial work will be high and is increasing;
• the skilled staff needed to tackle the problem are in high demand and short supply;
• most organisations have yet to establish a realistic budget for their year 2000 project;
• priority needs to be given to the preparation of contingency plans;
• opportunities exist to improve the co-ordination of effort and co-operation between authorities and trusts, including dissemination of ideas, good practice and compliance status information; and
• building and maintaining public confidence is a crucial part of protecting the systems of authorities and trusts.

The problems faced are not insurmountable but will require considerable effort to resolve. Organisations must ensure that they are prepared. This paper highlights the key issues that management should address as well as the risks and consequences associated with each. We identify the questions that members, managers and non-executive directors should ask about their own organisation's preparedness. These are drawn together in a self-assessment questionnaire in a centre pull-out section.

The actions recommended in this paper are intended to help authorities and trusts reduce the risk of significant problems with their systems as a result of the year 2000. It is for the management of authorities and trusts to assess the applicability of the paper's recommendations to their own local circumstances.
Introduction

Why the Audit Commission has written this paper

1. In the early days of computing, data storage and computer memory were expensive. Efficient programming practice encouraged the use of two rather than four digit fields to record dates, and this became an industry standard. So '1986' became '86'. Many systems still adopt this format and could fail or produce erroneous results when attempting to perform calculations involving the year 2000 or beyond.

2. The problem, however, is not confined to computers and computer systems. Much of the equipment we see around us and use contains, or is controlled by, a microchip, which may use date and time information to function effectively. Medical equipment, passenger lifts, traffic lights, central heating boilers and car park barriers are examples of equipment which could be affected.

3. The millennium date change presents managers in both the public and private sectors with a major challenge – probably one of the biggest challenges that they have faced in recent years. The scale and complexity of the problem, coupled with the possible consequences should projects fail, means that the year 2000 project must be given the highest priority.

For whom?

4. The year 2000 project must also be viewed in the context of the significant changes that are taking place within public sector bodies. Issues such as the NHS White Paper and the changes resulting from local government re-organisation and best value continue to require the attention of management. The demands of year 2000 will place managers under even greater pressure.

5. However, the deadline for the project cannot be moved. If services are not to be disrupted, organisations should, by now, have established a formal year 2000 project, identified the risks that they face and be taking appropriate action to deal with them.

6. A key factor in influencing the rate of progress is the extent to which there is ownership and management of the problem at board level. The Audit Commission has written this paper to help top management in local government and the NHS to understand better the implications of the date change for their operations and the action that they should take to ensure that the risk of serious failure is minimised. This paper is timely, coming when the focus of many projects must change from awareness to action.

The work upon which this paper is based

7. Since January 1997, auditors from District Audit have assessed year 2000 preparations at around 350 local authorities, NHS trusts and other audited bodies (referred to as authorities and trusts throughout this paper). Progress has been reviewed at:

- 145 London boroughs, metropolitan, district, county and unitary councils;
- 174 acute, community and ambulance trusts and health authorities; and
8. Our findings are based upon the latest reviews – that is, for the six months to March 1998 – and have been confirmed by results from other recent surveys such as the Local Government Association and Zurich Municipal, the NHS Confederation evidence to the Parliamentary Committee on Science and Technology and the NOP survey commissioned by the Computing Services and Software Association, the trade association for the software and Information Technology (IT) services industry.

**What the Commission is doing**

9. The Commission’s auditors continue to review the preparedness of authorities and trusts and are scheduled to do so through to the year 2000 and beyond. Revisits to authorities and trusts to monitor their progress since the last review and against best practice benchmarks are already under way.

10. There is a wealth of sound advice and good practice material on the year 2000 issue produced by national and regional groups and by individual authorities and trusts. Since all organisations are tackling similar issues, it is important that information is shared. This management paper is part of the process and the Commission will continue to share good practice and encourage action where required.

11. The paper is divided into a series of sections, providing information about year 2000 issues and suggested action. At the end of each section, we have summarised:

- the risks and consequences of failing to take action;
- indicators of success that chief executives could look for within their own organisation; and
- the progress which authorities and trusts have made in tackling the problem.

12. Progress has been compared against a series of benchmarks. These are also drawn together, at the centre of the paper, in a self-assessment questionnaire which is designed to be pulled out, copied and distributed throughout the organisation.

**Acknowledgements**

13. This paper was written by Keith Dixon, Associate Director with District Audit (DA), and is based upon the detailed work undertaken by DA staff throughout 1997 and 1998. The results were reviewed by an advisory group (see Appendix 2 for the membership of this group). The Audit Commission is grateful for their assistance. Responsibility for the contents and conclusions of this paper rests solely with the Audit Commission.

Thanks are also due to those organisations which have provided examples of current practice.
1. The millennium date problem

What could go wrong?

14. So what could go wrong? Problems could arise before, during or after the millennium unless corrective action is taken. Some problems have already occurred [BOX A]. Delivery of public services could be disrupted. For example:

- medical equipment malfunctions may present a risk to health and life if devices deliver or calculate incorrect treatment doses or if life-support equipment ceases to function;
- accounting software may be unable to cope with the 99/00 financial year starting on 1 April 1999;
- lifts may cease to function where an embedded system calculates – incorrectly – that a service is long overdue;
- patient recall systems in GP practices could fail to accept dates beyond 1999;
- vehicle fleet maintenance systems may refuse to accept the entry of new vehicles because the lease period associated with the vehicle extends beyond the year 2000; and
- authorities may be unable to collect income due to a failure of their revenue systems.

15. NHS acute trusts face the highest risk, since they have the largest number of critical procedures such as theatre scheduling, hospital admissions and prescribing. They also possess the greatest number of medical devices, many of which could contain embedded systems, a particular area of risk. General practitioners also make use of a wide variety of hardware and software and will need help in dealing with year 2000 issues.

16. Organisations will also need to be fully aware of the legal implications of the year 2000 and potential problems that could arise. These fall into two main categories:

- contractual relationships and obligations with suppliers, customers and employees; and
- duties under such legislation as Health and Safety and Consumer Protection Acts where non-compliance is a criminal offence. Penalties can range from fines to imprisonment.

[BOX A]

Year 2000 problems are already happening

At one local authority the computer system, which controls the issue of Orange Badges to people with disabilities, no longer operates as it was designed to do. The authority normally issues the badges for a three-year period but the system does not accept an expiry date beyond the year 2000.

One NHS trust reverted to making appointments for patients manually because its patient administration system is not yet year 2000 compliant. The system will not allow the booking of appointments with a date of 2000 or beyond.

Source: District Audit
17. The problems are not insurmountable, but they will require considerable effort to resolve. There are no quick-fix solutions, but a systematic approach and a properly constituted and resourced project can help to minimise risk. Those organisations which made an early start to their year 2000 preparations may have time to resolve some of the less critical issues. Those that started much later may only have sufficient time to tackle key areas of activity.

Why might these problems occur?

Dates
18. For many years it has been common practice to store dates in a format which includes only the last two digits of the year – for example, 22/12/86. The assumption is that the year is 1986. As the millennium approaches this may no longer be valid and problems could arise as the year 2000 and later years are taken into account. The main difficulty is that although the year 1999 is followed by 2000, the opposite is true when considering these years in two digit number terms – that is, 00 precedes 99.

19. An added complication is that the year 2000 is a leap year. Some systems, it is reported, are incorrectly programmed to deal with leap years and could consequently fail to operate on 29 February 2000 or 31 December 2000 – that is, the 366th day that year.

20. Problems are already evident in some systems. Those that rely on processing future dates are particularly vulnerable. A major company's stock control system rejected a consignment of tinned food, the 'sell by' date of which was beyond the year 2000. It calculated that the contents were over 90 years old.

21. In some systems, 9 September 1999 could cause problems or, to be more accurate, its numerical equivalent – 9999. This may have been used by programmers to denote an end of file or a default value in a data entry screen which, when encountered, could cause the system to fail.

Computers and systems
22. Such date-related problems can affect the computer itself or the software running on it, causing the system to fail or to process information incorrectly [BOX B].

Embedded systems
23. Problems resulting from the incorrect processing of dates in computer systems are relatively easy to grasp. However, the date change problem goes beyond computer hardware and software [EXHIBIT 1]. It extends, potentially, to any equipment which is controlled, monitored or assisted in its operation by an embedded system. In its simplest form, such a system may be a single microprocessor, a 'chip'.

---

BOX B

An example of what could go wrong

The following components of a system running on a PC could be affected by date problems:

- the internal clock in the PC itself;
- the mechanism which controls the operation of the various PC components;
- the operating system;
- the application package – for example, spreadsheet software; and
- the individual application – for example, a specific spreadsheet.

Source: Audit Commission
24. Embedded systems are used extensively in facilities such as lifts, car park barriers, heating systems, video recorders and medical equipment. Affected equipment can be difficult to identify since the presence of the embedded system may not be obvious even to a trained observer. Some systems may also be extremely difficult to locate or test – for example, those used to regulate the flow of oil in pipelines in the North Sea!

25. The year 2000 project manager at one NHS trust is quoted as saying:

'The problem extends to all areas of the hospital – lifts, diagnostic equipment, X-ray machines, anaesthetics, breathing equipment and monitors.'

How large is the problem?

26. During 1995, more than 200 million PCs were sold worldwide. In 1996, about 7 billion embedded systems were distributed. Recent research has indicated that around 5 per cent of simple embedded systems failed when tested. For more complex systems, failure rates of between 50 per cent and 80 per cent are reported.

27. Furthermore, there are several major microchip programming languages, each with its own variant used in embedded systems. It is therefore possible for
apparently identical pieces of equipment to behave differently because the internal components come from different sources.

28. Anthony Parish, Director General of the Federation of Electronic Industries has said:

'There is no doubt about it – embedded systems is the nasty one ...there are 50 to 100 times more embedded microprocessors than there are in IT systems.'

29. Neither is there any experience of similar projects that authorities and trusts can draw upon. The year 2000 project is quite different from any that organisations have undertaken before:
- every other organisation is working on the same project and to the same deadline;
- the deadline is fixed and cannot be moved; and
- there are many interdependencies – meaning that a failure in someone else's system can seriously affect services elsewhere.

30. Because everyone is tackling the problem simultaneously and working towards the same end date, available resources to fix the problem will be scarce. These factors and the consequences of failures in critical systems place the year 2000 project in the extremely high-risk category.
2. What can be done?

31. There are many potential problems, but it is not yet too late to take action. It is possible that management can reduce the risk of failure and minimise the impact of any disruption to services. A culture of openness about preparations and a willingness to share information with other organisations is also essential.

32. From our work at authorities and trusts, and from current best practice, we have identified seven steps that organisations should take [EXHIBIT 2]. These actions are not sequential and should, in some cases, be undertaken in parallel. For example, raising and maintaining awareness of year 2000 issues should run throughout the whole project.

33. The rest of this paper contains a section for each step in which we consider:

- the action required in more detail;
- examples of good practice from authorities and trusts;
- an overall picture of progress;
- an outline of risks; and
- some suggested measures that could provide chief executives with an indication of whether successful action has been taken.

EXHIBIT 2
Action points

There are seven key steps that organisations should take to prevent failure of key services and critical equipment.
Overall progress

34. The Commission's auditors have been reviewing year 2000 preparations by authorities and trusts since January 1997. The objective of the reviews has been to assess progress by authorities and trusts against key project milestones and to share good practice. Each authority has received a report on its progress which recommends appropriate action. This has been discussed and agreed with management.

35. A series of benchmarks [BOX C] has been used by auditors to measure the progress made by individual authorities and trusts. The benchmarks also appear in the progress summaries at the end of each section. They have been refined on the basis of the reviews undertaken at some 350 sites and will be updated on a regular basis. Auditors used a simple scoring mechanism to provide a quantitative view of their assessment of progress [BOX D].

36. We have also taken account of targets set by others. The NHS Executive (NHSE) established explicit project targets for trusts and health authorities in its letter, EL 97(59), in October 1997. These are:

- complete initial project plans by 30 November 1997;
- prepare detailed project plans including contingency plans, detailed inventory and budget estimates by 31 March 1998; and
- all critical systems to be ready and fully tested, or have developed detailed plans for coping without systems or equipment that cannot be repaired or replaced, by 31 December 1998.

37. The Welsh Office has written to NHS organisations in Wales. The Local Government Management Board has recommended action by local authorities.

38. We have used the benchmarks to provide a self-assessment questionnaire which senior managers could apply to their own year 2000 projects. The questionnaire appears at the centre of this paper.

BOX C

A mid-term check on progress

Did we reach these milestones by March 1998?

- senior management fully briefed;
- regular communication throughout the organisation established;
- strategy formulated for dealing with the problem;
- suitable project sponsor appointed;
- risk assessment undertaken;
- multidisciplinary project team operating;
- detailed project plan developed;
- estimated budget prepared;
- inventory of critical systems complete;
- business partners identified and contacted;
- software licence problems identified;
- critical systems and equipment identified and priorities determined;
- year 2000 compliance included in purchasing specifications;
- contracts reviewed;
- testing plan formulated;
- testing commenced; and
- realistic target set for completion of contingency plans.

Source: District Audit
**BOX D**

How auditors assessed progress
At each site visited, the auditor used the following scoring mechanism to provide a measure of progress for reporting to authority or trust management.

<table>
<thead>
<tr>
<th>Score</th>
<th>Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No project sponsor appointed</td>
</tr>
<tr>
<td>1</td>
<td>Sponsor appointed but not sufficiently senior</td>
</tr>
<tr>
<td>2</td>
<td>Sponsor at board level appointed</td>
</tr>
<tr>
<td>3</td>
<td>Sponsor at board level appointed with power to authorise resources and finance</td>
</tr>
</tbody>
</table>

**EXAMPLE:**

HAS A SUITABLE PROJECT SPONSOR BEEN APPOINTED?

<table>
<thead>
<tr>
<th>Score</th>
<th>Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No project sponsor appointed</td>
</tr>
<tr>
<td>1</td>
<td>Sponsor appointed but not sufficiently senior</td>
</tr>
<tr>
<td>2</td>
<td>Sponsor at board level appointed</td>
</tr>
<tr>
<td>3</td>
<td>Sponsor at board level appointed with power to authorise resources and finance</td>
</tr>
</tbody>
</table>

**EXHIBIT 3**

Progress compared with key project milestones

All types of authorities and trusts are behind schedule with their year 2000 projects.

![Progress score chart](chart)

Source: District Audit

39. District Audit had undertaken some 200 reviews in the six months to March 1998. In each case, the auditor's assessment of progress made, compared with the benchmarks appropriate at the time of the reviews and agreed with management, has been used to provide an overall indicator of progress by authority type [EXHIBIT 3].

40. This overall indicator represents the average position for each type of authority and trust and includes, therefore, organisations that are making good progress as well as those that are not. The self-assessment questionnaire is designed to help authorities and trusts to decide where their own year 2000 projects are in relation to the benchmarks.
41. We have also analysed auditors’ assessments across seven key project areas and have concluded that action is required in each area of the year 2000 project [EXHIBIT 4].

42. The key message is that, in general, all groups of authorities and trusts are behind schedule with their year 2000 projects. There is still time to resolve problems provided management takes the appropriate action. The Audit Commission will be encouraging auditors to monitor progress and will provide update reports on their findings at regular intervals.

43. The next few sections consider, in more detail, the key actions that management should take and report the progress that authorities and trusts have made in each area.
3. Raise awareness

44. The first step in securing commitment and resources is a high degree of awareness throughout the organisation. This is particularly true for senior management. Authorities and trusts must ensure that the project is owned at a high level by getting the management board to recognise the problem.

45. Staff are likely to be aware of the problem but not all may understand the full implications for the organisation as a whole or for their particular department. Some may be mistaken about the potential risks. Authorities and trusts should plan to inform staff throughout the organisation of the problems faced and the action that management is taking [BOX E]. Awareness sessions for staff, together with a programme of regular updates on the year 2000 project will help to increase understanding.

46. Publishing a year 2000 newsletter and making information packs available in all departments, such as those provided by the NHS Executive Year 2000 Programme or the Action 2000 teams, are other useful options.

47. Managers should also ensure that year 2000 issues are built into staff plans and objectives. Staff should be encouraged to consider the implications of date problems upon their own areas of work and useful information captured and passed to the project team.

48. Some authorities and trusts have established a programme of events designed to raise the awareness and understanding of year 2000 issues within the organisation and the wider business community [CASE STUDY 1, overleaf].

49. Media interest in the year 2000 is increasing and will continue as 2000 approaches. Authorities and trusts will need a public relations strategy to manage public concerns. Building public confidence will be vital. For the general public, management should ensure that PR teams are fully aware of the problems and what is being done about them. Articles in the local press and presentations to local committees, community health councils, or schools should be considered.

BOX E

Staff awareness

Information that managers could make available throughout the organisation includes:

- description of the problem and its effects;
- project sponsor and team members;
- key project stages, milestones and dates;
- progress to date;
- plans for the future;
- techniques being used;
- things that staff should and should not do;
- compliance information by product;
- World Wide Web addresses containing helpful year 2000 material;
- best practice; and
- suggestions/reporting facility.

Source: Audit Commission
CASE STUDY 1

Taking a wider perspective
Cornwall County Council has taken the following steps to raise awareness and understanding of year 2000 issues throughout the county area:

- flyers entitled Year 2000 – Making IT Switch to the New Millennium were distributed on a monthly basis to each member of staff with the Council’s in-house magazine;
- seminars were organised for county staff to increase awareness of year 2000 issues;
- staff from district councils were also invited to a series of seminars;
- close working relationships were established with other counties and public bodies; and
- useful links with local businesses and business organisations have been forged.

<table>
<thead>
<tr>
<th>WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Awareness</strong></td>
<td></td>
</tr>
<tr>
<td>- senior management has been fully briefed and kept up to date</td>
<td></td>
</tr>
<tr>
<td>- the nature and size of the problem has been communicated throughout the organisation</td>
<td></td>
</tr>
<tr>
<td><strong>WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998</strong></td>
<td></td>
</tr>
<tr>
<td><strong>PROGRESS</strong></td>
<td></td>
</tr>
<tr>
<td>Although awareness of year 2000 issues is generally widespread, authorities and trusts must ensure that there is greater understanding of the implications for the organisation and service delivery.</td>
<td></td>
</tr>
<tr>
<td>Four-fifths of authorities and trusts have provided briefings for senior management.</td>
<td></td>
</tr>
<tr>
<td>Consideration should be given to communicating about the scope of the problem through newsletters, workshops, staff newspapers, etc, throughout the organisation.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MANAGEMENT CHALLENGES</th>
<th>so that you minimise the risk of...</th>
<th>and benefit from...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You should ensure that you have...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fully briefed senior management</td>
<td>lack of ownership at the highest level</td>
<td>taking risks seriously</td>
</tr>
<tr>
<td>informed staff of the problems faced and kept them up to date with year 2000 issues</td>
<td>lack of staff motivation and an unwillingness to co-operate</td>
<td>identifying critical systems</td>
</tr>
<tr>
<td>a strategy for informing the public</td>
<td>uncertainty and misconceptions about what is being done</td>
<td>public confidence and no adverse comment in the media</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHIEF EXECUTIVE’S INDICATORS OF SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attendance numbers at seminars</td>
</tr>
<tr>
<td>Contributions of information from staff</td>
</tr>
<tr>
<td>Number of top managers directly involved in project</td>
</tr>
<tr>
<td>Direct reporting line to the board for year 2000 project manager</td>
</tr>
</tbody>
</table>
4. Establish the project

50. The year 2000 project is high risk and has a fixed deadline. Good project management will be critical to its success. Historically, the absence of such arrangements has been one of the main causes of project failure.

51. A workable and effective structure should include the appointment of a project steering group, project manager and project team. Someone at board level should be given personal responsibility for sponsoring the project. They should chair the steering group, report progress to the board and have sufficient authority to authorise the allocation of resources and finance to the project. The project should feature regularly on board agendas and be actively discussed.

52. A project manager who possesses the necessary skills and experience is required to manage and lead a project of this importance. The manager must command the trust and respect of the board and have ready access to board members.

53. The year 2000 project must cover equipment controlled by embedded systems as well as computers and information systems. While the project team may be managed by the organisation’s IT department, it is essential that embedded system issues are not overlooked. Appropriate technical and professional expertise should be included in the project team. The Institution of Electrical Engineers (IEE) advocates the appointment of an embedded systems manager and team.

54. For those organisations that have adopted a devolved approach to the provision of IT, departmental barriers may need to be overcome. It is important that major departments are represented on the project team [BOX F]. However, there should be one project sponsor and proper central co-ordination of the project across the whole of the organisation. Year 2000 projects should be independently reviewed and progress monitored on a regular basis.

BOX F

Establishing the proper project arrangements: example of an NHS trust project structure

Source: District Audit
55. The NHS Executive has issued guidance for health authorities and trusts advising them that the year 2000 problem should be treated as the highest non-clinical priority. The Welsh Office has issued similar guidance. NHS chief executives were advised that:

- they are accountable for all problems in their organisations resulting from year 2000;
- the chief executives of heath authorities are responsible for co-ordinating year 2000 work in the primary care sector; and
- NHSE regional offices are instructed to monitor the progress of projects.

56. A project plan is necessary and should provide key milestones against which the progress of the project can be measured [CASE STUDY 2]. A project budget will be essential, but it may be impossible to be accurate about total project costs in the early stages. The full implications may become known only once the project is under way. Appropriate reporting and monitoring procedures should also be established.

**CASE STUDY 2**

An extract from a project plan

The first phase of Cornwall County Council's project consisted of an awareness campaign and scoping exercise. It started in April 1997 and was completed in November 1997. The second phase commenced in January 1998 and is planned to be completed by February 1999.
57. The project plan should identify the staff resources required to undertake each stage of the project. Authorities and trusts will need to ensure that key staff and contractors have contracts which ensure that they are employed up to the completion date for the project and beyond to deal with any subsequent problems. Guidance will be required to cover any work that is necessary outside normal staff contracts. Authorities and trusts should also take steps to minimise the risk of losing key staff. Some organisations have introduced pay incentives for those who stay beyond the millennium.

<table>
<thead>
<tr>
<th>WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project formation</strong></td>
<td>Less than one-third of authorities and trusts have documented their strategy for dealing with the problem. Project teams have been established but in some cases no project sponsor has been appointed.</td>
</tr>
<tr>
<td>• the organisation has a strategy for dealing with the year 2000 problem</td>
<td>In local government the majority of project teams are IT-based. Project team membership in the NHS is more representative of the whole organisation.</td>
</tr>
<tr>
<td>• a suitable project sponsor has been appointed</td>
<td>Around two-thirds of authorities and trusts have estimated the staff resources they will require to fulfill the project. There are concerns at chief officer level that the appropriate skills are in short supply.</td>
</tr>
<tr>
<td>• the project team includes representatives from departments across the organisation, not just from IT</td>
<td>One-third of authorities and trusts have made specific budgetary provision for Year 2000. Some plan to use IT and equipment replacement budgets. Some are still considering the scope of the problem that they face.</td>
</tr>
<tr>
<td>• adequate budgetary provision has been made</td>
<td>Progress on embedded systems is understandably much slower than for IT and IT systems. Estimates for fixing embedded system problems are not yet available.</td>
</tr>
<tr>
<td>• staff resources have been identified and are available</td>
<td>Fifty per cent of authorities and trusts have established formal mechanisms to flag and manage potential problems. As the next, critical, stage of the project is reached, authorities and trusts will need to give more detailed thought to risk management.</td>
</tr>
<tr>
<td>• formal mechanisms are in place to flag up potential problems</td>
<td></td>
</tr>
</tbody>
</table>
### MANAGEMENT CHALLENGES

<table>
<thead>
<tr>
<th>You should ensure that you have...</th>
<th>so that you minimise the risk of...</th>
<th>and benefit from...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a project sponsor at board level</td>
<td>lack of commitment at top level</td>
<td>giving the project priority and resources</td>
</tr>
<tr>
<td>a project steering group</td>
<td>lack of recognition of the wider business implications of the changes</td>
<td>develop solutions that fit the business</td>
</tr>
<tr>
<td>a project team with clearly defined objectives</td>
<td>an ad hoc approach</td>
<td>integrating developments and solutions</td>
</tr>
<tr>
<td>a rigorous monitoring process to track progress</td>
<td>slippage</td>
<td>keeping the project on track</td>
</tr>
<tr>
<td>key milestones for the project</td>
<td>important elements of the project being overlooked</td>
<td>no failures in key service areas</td>
</tr>
<tr>
<td>an estimate of the staff resource requirements</td>
<td>project being under-resourced</td>
<td>keeping the project on time</td>
</tr>
<tr>
<td>a budget for the project</td>
<td>insufficient funding for the project</td>
<td>successfully implementing solutions</td>
</tr>
<tr>
<td>a mechanism for identifying potential problems</td>
<td>failing to manage the risks</td>
<td>reducing the risk of potential liabilities</td>
</tr>
</tbody>
</table>

### CHIEF EXECUTIVE’S INDICATORS OF SUCCESS

- Project plan with key milestones, tasks and subtasks
- Realistic timescales included
- Resource requirements that can be substantiated
- Risk management plan in place with risks managed by accountable people
- Assurance that key staff are retained for the life of the project
- Favourable project assurance reports
5. Scope the problem

58. Authorities and trusts should establish an inventory of systems and equipment and collect the necessary information about each [APPENDIX 1]. Where third party software or equipment is involved, it will be necessary to make contact with suppliers and business partners to determine plans for achieving conformity with compliance standards.

59. Where possible, a joint approach with other organisations should be adopted to reduce duplication and effort.

60. Some suppliers have been reluctant to give assurances, while others have published plans and dates by which their products will be compliant. It is essential that any responses received from suppliers are carefully examined to ensure that they are clear and unambiguous. Authorities and trusts will also wish to distinguish between:

- **readiness** – works well enough; and
- **compliance** – works in every way.

For some systems a state of readiness may be sufficient. Equipment and information systems may not need to be compliant as long as they provide an acceptable level of functionality. For example, manually advancing the date may be a reasonable solution in some instances.

61. Compliance may mean different things to different people. In order to avoid any confusion, a standard definition of year 2000 compliance, such as the British Standards Institution (BSI) definition PD2000-1, should be used as the basis for discussions with suppliers [BOX G].

*Where possible, a joint approach with other organisations should be adopted*

---

**BOX G**

**A year 2000 compliance standard**

Organisations should use a standard definition to avoid any confusion.

Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during, or after the year 2000.

In particular:

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

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

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

Rule 4. Year 2000 must be recognised as a leap year.

*Source: BSI*
62. Where assurances have been given by third parties, these should be documented and evidence of the tests and results obtained and kept. For critical information systems, organisations should also carry out their own tests. In one instance, a software package which had been certified by its supplier as year 2000 compliant was subjected to tests by IT staff. Significant problems were detected, causing the early termination of testing.

63. If a software supplier ceases to trade or is unable to support the system, it may be possible, where an escrow agreement* is in place, for authorities to obtain and fix the software themselves. However, they can be very difficult to enforce and of little help if proper documentation is not available.

64. However, where pursuing an escrow agreement is an option, authorities must ensure that they obtain the correct source code and compilers for the system and that they have access to appropriate programming resources. The National Computing Centre (NCC) has launched a year 2000-specific software escrow service, which should help users to reduce some of the uncertainties. Where this is not an option, authorities and trusts should plan to replace their systems.

65. Information on compliance status or the plans of suppliers to achieve it in respect of specific products is beginning to emerge – albeit slowly. There is a need to ensure that this information is shared and authorities and trusts are encouraged to contribute to national databases which are making information available on the World Wide Web. Organisations should also consider what other forms of self-help are possible. For example, unitary councils in Wales have formed a Millennium Club [BOX H].

66. There is clear evidence that year 2000 work is the subject of much local reinvention. Strong central support is required in key areas, particularly liaison with suppliers, contingency planning and the testing of widely used systems. The NHS Executive Year 2000 Programme, for example, is undertaking a similar role in the NHS. However, until recently, there has been little centrally co-ordinated effort on behalf of local government.

---

**BOX H**

Co-ordination of year 2000 effort

The Millennium Club in Wales is a good example of how self-help can work:
- all unitary authorities are participating;
- year 2000 presentations are being given in each council;
- a common project methodology has been adopted;
- the Club has met quarterly;
- inventories have been exchanged;
- compliance databases are being developed;
- letters to suppliers have been drawn up;
- details of testing undertaken so far are being shared; and
- a club website is being established.

*Source: District Audit*

---

* Escrow agreements guarantee the availability of the program source code.
A Stitch in Time

Questions for the chief executive, chief officer team, members and boards

Please pull out and copy

In its management paper, A Stitch in Time, the Audit Commission identified a number of year 2000 issues for chief executives, chief officer teams, members and boards. They have been translated into a series of questions that can help you to assess your own level of preparedness.

The greater the number of statements that you can answer, the better your progress is likely to be. Those questions which result in a negative response, or a 'don't know' answer, could well indicate areas where action is required.
<table>
<thead>
<tr>
<th><strong>Question</strong></th>
<th><strong>Evidence</strong></th>
</tr>
</thead>
</table>
| When was top management last briefed about the year 2000 problem, the effects upon the business and the progress being made in resolving the problem? | Last briefing  
Next briefing                                                                 |
| Who is sponsoring the year 2000 project?                                   | Name  
Position                                                                 |
| What is the project structure and who are the key players?                 | Attach organisation chart  
Key players                                                                             |
| When was the detailed project plan approved?                               | Date of approval by steering group                                             |
| How often is progress against the plan monitored and reported and by whom? | Frequency  
Name                                                                                           |
| How many PCs do we have in our organisation? How many networks? How many pieces of equipment containing embedded systems? | PC number  
Network number  
Embedded systems number                                                             |
| What budget have we established for fixing the problem?                   | £                                                                                           |
| What skills and resources do we have in-house to fix the problem and manage the project? | IT skills  
Management  
Engineering  
Other                                                                 |
<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>When do year 2000 staff contracts run out?</td>
<td>Dates</td>
</tr>
<tr>
<td>Who will take over if the project manager leaves?</td>
<td>Name</td>
</tr>
<tr>
<td>Which of our systems and equipment take priority?</td>
<td>List</td>
</tr>
<tr>
<td>Which of our systems and equipment must wait?</td>
<td>List</td>
</tr>
<tr>
<td>Who is charged with preparing our contingency plan and by what date?</td>
<td>Name, Date</td>
</tr>
<tr>
<td>Which compliance standard has been adopted in our amended purchasing guidelines so that we don't acquire non-compliant hardware, software or equipment?</td>
<td>Standard</td>
</tr>
<tr>
<td>Our main business partners have assured us that they will be year 2000 compliant by the dates shown</td>
<td>Supplier, Date</td>
</tr>
<tr>
<td>What percentage of suppliers have we sought assurances from about the compliance of their hardware, software or equipment?</td>
<td>per cent so far</td>
</tr>
<tr>
<td>Question</td>
<td>Evidence</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>What percentage of those contacted have responded unambiguously so far?</td>
<td>per cent so far</td>
</tr>
<tr>
<td>What are the 'high' risks recorded in the risk register and who is responsible for their management?</td>
<td>Risk Name</td>
</tr>
<tr>
<td>Who is ensuring that we protect ourselves from legal challenge?</td>
<td>Name</td>
</tr>
<tr>
<td>How have we communicated year 2000 issues to the rest of the organisation?</td>
<td>How</td>
</tr>
<tr>
<td>Who is handling public concerns about year 2000 issues?</td>
<td>Name How</td>
</tr>
<tr>
<td>What percentage of our assets have been tested so far for year 2000 compliance?</td>
<td>PC per cent Hardware per cent System software per cent Networks per cent Software applications per cent Equipment per cent</td>
</tr>
</tbody>
</table>
Each authority or trust could potentially be seeking information about the status of equipment or software from the same suppliers. There are opportunities for improved co-ordination, dissemination of information and negotiation with major suppliers in order to bring about a speedy resolution of outstanding compliance issues. In our view the bodies best placed to manage such processes are:

- the NHS Executive Year 2000 Programme for major NHS IT supplies;
- the NHS Supplies Authority for major supply contracts;
- NHS Estates for NHS property-related embedded systems;
- in Wales, the equivalent organisations and consortia which have been established for those specific purposes;
- the Medical Devices Agency for medical equipment;
- the Local Government Association for English local authorities; and
- the Millennium Club for local authorities in Wales.

### WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998

**Scope the problem**

- an inventory covering IT, equipment and contracts has been compiled
- suppliers have been contacted to establish compliance status
- ambiguous responses are being followed up
- software licence problems have been identified
- the date format requirements of external agencies have been identified

### PROGRESS

Over one-third of authorities and trusts have yet to complete an inventory of IT, equipment and contracts and collect the basic information that they need. District councils as a group are lagging behind the rest.

Assurances about compliance of products are being sought from suppliers. Software suppliers were among the first group to be contacted. Progress in contacting manufacturers of embedded chip equipment is not as advanced.

Information from suppliers is still incomplete and some manufacturers have not yet issued compliance statements. Consequently there has been little opportunity to test the validity of responses. There are real concerns within some trusts that compliance questionnaires sent to major suppliers of medical equipment remain unanswered.

More work is required to establish the extent of software licence problems, as this will be a necessary prerequisite to testing.

Databases of compliance information about IT and non-IT products are being developed – for example, the NHSE for the NHS and the Society of Information Technology Management in the local government arena. All organisations are encouraged to share information for the advantage of all.
### MANAGEMENT CHALLENGES

<table>
<thead>
<tr>
<th>You should ensure that you have...</th>
<th>so that you minimise the risk of...</th>
<th>and benefit from...</th>
</tr>
</thead>
<tbody>
<tr>
<td>compiled an inventory and collected the basic information about affected IT and equipment</td>
<td>lack of understanding of the scale of the problems</td>
<td>identifying key systems or equipment</td>
</tr>
<tr>
<td>contacted suppliers</td>
<td>not knowing whether to fix or replace</td>
<td>choosing the most cost-effective solution</td>
</tr>
<tr>
<td>tested suppliers' responses</td>
<td>non-compliance</td>
<td>hardware, software or equipment that is already compliant</td>
</tr>
<tr>
<td>reviewed software licences</td>
<td>software failure</td>
<td>preventing delay of the testing programme</td>
</tr>
</tbody>
</table>

### CHIEF EXECUTIVE'S INDICATORS OF SUCCESS

- Confirmed inventory
- Tracking of supplier responses
- Compliance-status tracking
6. Decide priorities

68. Given the scale of the task facing authorities and trusts, it is already evident that it may not be possible to make all systems and equipment year 2000 compliant by the required deadline. In any event this may not be a sensible goal. The objective should be to ensure a managed transition across the millennium that does not put services at risk. Critical systems and equipment should be identified to ensure that resources are allocated to them. Prioritisation is essential.

69. Establishing priorities requires an assessment of the impact that the problem is likely to have on people, services and the business. What risk is there that the system could fail? What will be the effect if it does? Some application systems are more critical to the delivery of services than others—for example, the provision of benefits. Other equipment, particularly medical equipment, may pose a risk to health if a malfunction occurs. Consideration of these issues must clearly receive the highest priority.

It is already evident that it may not be possible to make all systems and equipment compliant by the required deadline

70. A critical failure may be defined as one which would prevent service delivery or the safe or legal functioning of the organisation. A minor failure would be a source of irritation or inconvenience. A more detailed model, based upon an Australian standard [BOX I], could help organisations to decide where action is required and what must wait.

71. Authorities and trusts should review their plans to determine whether earlier implementation of scheduled changes could obviate repairs to existing systems. The volume of change to systems is likely to be greater than normal and existing change control arrangements will need to be sufficiently robust to cope with the increased demand. Management should also ensure that departments understand that it will not be possible to do everything, and that it is unlikely that sufficient resources will be available to carry out planned, routine changes to systems.

### BOX I

#### Risk management: an example based upon an Australian Standard

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
<th>Example of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>No injuries, low financial loss</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>First Aid Treatment, medium financial loss</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Medical treatment required, high financial loss</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Extensive injuries, loss of service, major financial loss</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Death, huge financial loss</td>
</tr>
</tbody>
</table>

Source: Australia/New Zealand standard 4360 – Risk Management
72. In relation to systems and equipment, authorities and trusts will be faced with a number of options:

- to fix those existing systems which will be required in the year 2000;
- to ensure that new systems are year 2000-compliant;
- to replace or decommission any systems or equipment that will become obsolete; and
- to provide a 'work around' where the impact is less critical.

In setting priorities, there are a number of questions that authorities could consider [EXHIBIT 5].

EXHIBIT 5

Prioritisation checklist

There are a number of questions that organisations may wish to consider when deciding what is critical.

- Is this application/equipment critical to the health and safety of staff and/or the public?
- Is this application/equipment critical to the day-to-day running of the business – for example, payroll, order processing, medical?
- Will failure or erroneous results from the application cause critical problems such as legal, non-compliance or wildly erroneous dates?
- Will failure or faulty results undermine management or merely inconvenience it?
- Are other applications or equipment dependent upon this application for the data it produces?
- Is the system/equipment provided by a third party and if so, do we know when a compliant version will be available?
- Is information from this system used outside the organisation?
- Will manual procedures enable us to work around any problem?
- Is the underlying platform year 2000-compliant – for example, database software?
- How will the asset be corrected?
- How long will it take to fix and how much will it cost?
- What fallback plans do we have in case of failure?

Source: District Audit
<table>
<thead>
<tr>
<th>WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prioritisation</strong></td>
<td></td>
</tr>
<tr>
<td>• systems and facilities have been prioritised according to:</td>
<td>Up to half of authorities and trusts have still to prioritise what needs to be done. The absence of full information about the scope of the problem should not prevent them from considering priorities.</td>
</tr>
<tr>
<td>– the impact of a malfunction</td>
<td></td>
</tr>
<tr>
<td>– the availability of suitable maintenance contracts</td>
<td></td>
</tr>
<tr>
<td>– links with other systems</td>
<td></td>
</tr>
<tr>
<td>– suppliers' plans for provision of compliant facilities</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MANAGEMENT CHALLENGES</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>You should ensure that you have...</td>
<td>so that you minimise the risk of...</td>
<td>and benefit from...</td>
</tr>
<tr>
<td>a sense of what needs to be done first and what must wait</td>
<td>critical tasks remaining untouched</td>
<td>key business processes being ready or compliant</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHIEF EXECUTIVE’S INDICATORS OF SUCCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority plan that identifies critical systems</td>
</tr>
<tr>
<td>Compliance strategy for each component</td>
</tr>
<tr>
<td>Priorities reflected in the overall project plan</td>
</tr>
</tbody>
</table>
7. Change procurement practices

73. It is unsafe to assume that all new equipment is year 2000-compliant. Out of a batch of ten new PCs tested by one local authority, only three proved to be compliant.

74. In order to avoid adding to an already significant problem, therefore, managers should ensure that hardware, software and equipment specifications as well as purchasing guidelines are altered to include compliance as an express written condition.

75. Software support and maintenance contracts should be reviewed. Some may only require the supplier to 'use reasonable endeavours' to rectify any fault. Any significant problems associated with the software at each of the customer sites could cause long delays for users.

76. Critical supply contracts that fall for renewal in 1999 should be reviewed closely. It may be advisable for them to be renewed early. In addition, authorities and trusts should review contracts under which they must provide a service.

77. Advice from legal staff should be sought on contractual matters of this nature.

<table>
<thead>
<tr>
<th>WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contracts and acquisitions</strong></td>
<td></td>
</tr>
<tr>
<td>• support and maintenance contracts have been reviewed to ensure that support in potential problem areas will be available</td>
<td>Two-thirds of authorities and trusts have taken appropriate steps to ensure that acquisitions are year 2000 compliant.</td>
</tr>
<tr>
<td>• purchasing guidelines have been altered to include compliance with year 2000 requirements</td>
<td>Only one-third have undertaken a thorough review of their existing support and maintenance contracts, or examined in any depth their critical business relationships and key interdependencies.</td>
</tr>
<tr>
<td>• hardware, software and equipment specifications have been altered to include compliance with year 2000 requirements</td>
<td>Authorities and trusts are urged to give these issues serious consideration as they should help to inform contingency planning.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MANAGEMENT CHALLENGES</th>
<th>You should ensure that you have...</th>
<th>so that you minimise the risk of...</th>
<th>and benefit from...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>reviewed your support and maintenance contracts</td>
<td>support not being available when needed</td>
<td>minimising any downtime</td>
</tr>
<tr>
<td></td>
<td>altered your purchasing guidelines and specifications</td>
<td>procuring non-compliant supplies</td>
<td>not adding to an already significant problem</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHIEF EXECUTIVE’S INDICATORS OF SUCCESS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amended service and supply contracts in place</td>
<td></td>
</tr>
<tr>
<td>Amended guidelines circulated</td>
<td></td>
</tr>
<tr>
<td>Amended specifications</td>
<td></td>
</tr>
<tr>
<td>Revised contract renewal programme</td>
<td></td>
</tr>
</tbody>
</table>
8. Test critical systems

To test or not to test?

78. The testing phase of the project could occupy half of the project resource. Planning for this phase is therefore vital.

79. The problem of testing embedded systems is particularly acute. The advice from the IEE is that testing such systems should be discouraged and undertaken only where there is no alternative [BOX J]. If information from a supplier is not forthcoming, or if it is felt that the supplier's information cannot be regarded as reliable, it may be necessary to perform tests.

80. Where testing is necessary, it should be undertaken only by a competent person and after suitable precautions have been taken. It is also necessary to recognise that attempting to test a device is to run the risk of rendering it incapable of being reset and therefore unable to function thereafter. Where no advice is received, clear instructions as to what should be done next are required – for example, the Medical Devices Agency should be informed if a piece of medical equipment is involved.

BOX J

Access to expert advice is needed when testing embedded systems

One local authority kept its staff aware of the year 2000 problem by publishing regular articles in a staff newspaper. One such article covered the problems associated with embedded systems. A caretaker decided on his own initiative to check the year 2000 compliance of the school's boiler system which, as a result, shut down. It took the authority one week to restart the boiler. Fortunately, the weather at the time was quite mild.

Source: District Audit

Dates and times

81. Dates and times are at the heart of the year 2000 problem. Testing for the existence of problems means that the equipment's system date and time will need to be reset to a point where problems could be expected to occur [EXHIBIT 6, overleaf]. Although most attention has been focused upon the first second of the new millennium, it should not be forgotten that other dates are potentially dangerous.

82. Problem dates can affect systems in the following ways:

• the system may fail to function correctly when a date-dependent operation is attempted which involves the problem date;
• the system may not function correctly subsequently; or
• it may not be possible to restart the system after the failure date.

83. Tests should therefore be designed to examine:

• the effects of rolling the date forward from one date to the problem date;
• whether system functions to be performed on a problem date will be performed correctly; and
• whether the next scheduled operation will be carried out correctly and at the right time.
EXHIBIT 6
The do's and don'ts of testing

There are a number of things that organisations should and should not do when testing critical systems.

<table>
<thead>
<tr>
<th>Do...</th>
<th>Don’t...</th>
</tr>
</thead>
<tbody>
<tr>
<td>· construct a detailed testing plan</td>
<td>· test embedded systems unless there is no alternative</td>
</tr>
<tr>
<td>· back up data and software on a variety of media before testing begins</td>
<td>· test without access to expert advice</td>
</tr>
<tr>
<td>· keep detailed records of the testing you have undertaken</td>
<td>· run tests on live operational systems</td>
</tr>
<tr>
<td>· make sure you can reset dates before rolling them forward</td>
<td>· assume your new PC is year 2000-compliant</td>
</tr>
<tr>
<td>· ensure that the testing environment is not linked in any way to the operational one</td>
<td>· invalidate your software licences by rolling forward dates</td>
</tr>
<tr>
<td>· get written assurances from suppliers</td>
<td>· damage security by rolling forward dates—for example, password expiry routines</td>
</tr>
<tr>
<td>· ask for and keep proof of testing undertaken by others</td>
<td>· assume that because a particular item has been successfully tested, all equipment of the same kind is also compliant</td>
</tr>
<tr>
<td>· print a hard copy of important information—for example, disaster recovery plans</td>
<td>· use test data which has not been aged past 2000</td>
</tr>
<tr>
<td>· check your insurance cover for losses caused by testing</td>
<td></td>
</tr>
<tr>
<td>· retest year 2000 changes if other amendments to systems are made</td>
<td></td>
</tr>
</tbody>
</table>

Source: Audit Commission

84. Users will know most about their systems and must, therefore, be available to help with testing. The year 2000 project team should make sure that users understand what is required of them. Sufficient time must be allowed for them to build test packs. Authorities and trusts should keep detailed records of time spent on testing, the tests undertaken and results, in case of future enquiries or year 2000-related problems.

85. Suppliers need to be informed of planned testing schedules so that they can provide compliant versions or planned upgrades of software before testing begins. Integrated testing should ensure that internal and external interfaces are all working properly.

86. Great care is required where testing involves rolling dates forward. Authorities and trusts should ensure that in advancing dates they do not unintentionally delete any archived data because the system calculates that the retention period of files has expired [BOX K].
87. Where the intention is to roll dates forward, those involved in testing should ensure that it is possible to roll them back again. It should also be remembered that advancing the system date could mean that a specific software licence is invalidated and, also, that the software may cease to operate. Rolling back the date in such situations will not work. The position should be checked with the software supplier before date changes are made.

88. NHS trust chief executives have expressed some concern over the resources that are required to undertake a thorough testing programme. Few feel that they have the expertise or resources to test any but the simplest systems. The NHSE year 2000 team is considering what part 'witness testing' – the practice of having tests on a commonly used piece of equipment or software witnessed and validated by an expert and the results made available – might play in the whole compliance programme. Regional offices of the NHSE year 2000 team are currently investigating how this could be organised.

89. Authorities and trusts should also clarify their position with regard to insured and uninsured losses before testing commences. Where consequential loss results from testing – that is, a specific action taken by the authority causes a failure in a system – reimbursement of the loss may be unlikely.
WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998

<table>
<thead>
<tr>
<th>Testing</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• a plan for testing has been prepared</td>
<td>Planning and undertaking the testing required has yet to start in earnest.</td>
</tr>
<tr>
<td>• potential testing problems are being identified for each system</td>
<td>It is unlikely, in our opinion, that the target date of 31 December 1998 (required by the NHS Executive for NHS organisations; advisable for local government) for completion of testing will be met.</td>
</tr>
<tr>
<td>• PCs have been tested</td>
<td></td>
</tr>
<tr>
<td>• assurances and proof of testing are being sought from manufacturers and/or suppliers of embedded systems</td>
<td></td>
</tr>
<tr>
<td>• third-party upgrades have been scheduled into the testing timetable</td>
<td></td>
</tr>
</tbody>
</table>

**MANAGEMENT CHALLENGES**

<table>
<thead>
<tr>
<th>You should ensure that you have...</th>
<th>so that you minimise the risk of...</th>
<th>and benefit from...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a co-ordinated approach to testing</td>
<td>a piecemeal approach to testing and implementation</td>
<td>confidence that key business areas are ready or compliant</td>
</tr>
<tr>
<td>a testing plan</td>
<td>damage to existing systems</td>
<td>secure information</td>
</tr>
<tr>
<td>started to test PCs</td>
<td>not enough time to complete critical tasks</td>
<td>more systems fixed and fewer manual alternatives</td>
</tr>
<tr>
<td>contacted suppliers of software and embedded systems</td>
<td>uncertainty about compliance of equipment</td>
<td>reducing the risk of failure or malfunction</td>
</tr>
</tbody>
</table>

**CHIEF EXECUTIVE’S INDICATORS OF SUCCESS**

- Detailed test plan for each system and component
- Evidence of tests undertaken by others
- Evidence of tests done in-house
- Test plans updated to accommodate other system changes
90. Despite all the efforts to solve the problem, it is possible that some organisations will experience service disruption before, after or on Saturday 1st January 2000. All organisations need a contingency plan to mitigate the effects of failure by ensuring that there is a plan of action for dealing with problems should they occur.

91. Organisations should, by now, have a clear idea of the process that they will go through and the people they need to involve in order to produce a plan. Emergency planning arrangements will also need to be reviewed and authorities and trusts must ensure that appropriate officers are involved and consulted when contingency plans are being developed.

**BOX L**

Recovery arrangements

The risk of simultaneous failures will need to be taken into account.

One company discovered by chance that its contingency plan, which included the hiring of a Portakabin to accommodate staff and vital business equipment such as PCs and siting it on the office car park, was identical to two other companies which shared the same office block. Unfortunately there was room for only one cabin in the car park.

*Source: Audit Commission*

92. In a normal situation, a typical contingency plan may involve replacing like with like. In a year 2000 context, however, this is inappropriate. For example, replacing a non-compliant system with an identical hardware platform and a back up of the same application is unlikely to provide a functioning system. Existing plans may also fail to address the implications of the higher risk of simultaneous failures in other organisations [BOX L].

93. The Monday following New Year's Day in 2000 will be a bank holiday and so, for many, the first day back at work will be Tuesday 4th January. This is an important consideration when planning to minimise the effect of a failure by having sufficient staff on duty.

Some NHS trusts are considering staff rotas for 31 December 1999 and are specifically planning to change staff over at midnight rather than 10.00pm to ensure that double the number of staff will be in the hospital at that critical time. Those organisations that are concerned about staffing levels over the New Year period and are considering working arrangements should consult staff as early as possible.

94. Someone else's problem could become yours. All organisations are affected by the year 2000 problem. Even though one organisation's systems are compliant, service disruption could still result because of a failure in the system of a third party supplier.
95. A failure in public services could impact upon the private sector. A failure in a local authority benefits system, for example, could lead to a housing association not receiving income on time and missing loan repayment dates to the Housing Corporation. Conversely, a failure in the production systems of a private-sector drugs manufacturer could have serious consequences for medical treatment in the NHS. Authorities and trusts should consider these issues carefully as part of their contingency planning, taking into account their business partners’ plans. There are a number of questions and issues that may be particularly relevant to year 2000 contingency plans which authorities and trusts will need to consider [EXHIBIT 7].

**EXHIBIT 7**

Contingency planning

Some questions are particularly relevant to year 2000 contingency planning.

**Staff**
- arrangements for key staff to be in work or on call over the New Year holiday;
- arrangements with suppliers, maintenance engineers and contract staffing agencies to have staff available in the event of problems;
- means of contacting key staff – for example, home telephone numbers, pagers, mobiles;
- alternative means of contact if telephones fail;
- transport for key personnel; and
- effective means of communicating with the public.

**Comfort factors**
- food provision – for example, it may not be possible to go to fast food outlets over the holiday period;
- heating and ventilation in the buildings where staff will be expected to work;
- suitable parking facilities;
- emergency power supplies;
- adequate water supply;
- crèche facilities; and
- cash available for emergencies.

**Equipment and related issues**
- alternative arrangements for key systems and equipment – for example, building access systems;
- variety of backup sources;
- permission to use software licences that restrict use to a particular site;
- emergency repair team available; and
- stocks of stationery that would normally be printed by the system.

Source: Audit Commission
<table>
<thead>
<tr>
<th>WHERE WE THOUGHT THE PROJECT SHOULD BE BY MARCH 1998</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contingency plans</strong></td>
<td></td>
</tr>
<tr>
<td>• the process for developing contingency plans is in place</td>
<td>Less than 10 per cent of authorities and trusts claim to have developed appropriate plans. This should be a priority in the next phase of the project.</td>
</tr>
</tbody>
</table>

**MANAGEMENT CHALLENGES**

<table>
<thead>
<tr>
<th>You should ensure that you have...</th>
<th>so that you minimise the risk of...</th>
<th>and benefit from...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a contingency plan</td>
<td>no back up if things go wrong</td>
<td>business continuity</td>
</tr>
</tbody>
</table>

**CHIEF EXECUTIVE’S INDICATORS OF SUCCESS**

Contingency plans covering key business processes and areas
10. How much will it cost to fix?

96. The Gartner Group estimates that the cost of locating, evaluating and reprogramming applications for year 2000 compliance may exceed $600 billion worldwide. Taskforce 2000 has estimated the cost for the whole of the UK as approaching £52 billion, of which the public sector’s bill is expected to be £12 billion.

97. There is no doubt that, for local government and the NHS, the cost of fixing the millennium bug will be large. Recent estimates provided to the NHS Executive by health authorities and trusts indicate additional year 2000 costs of approximately £330 million.

98. Sample costs for the healthcare sector were also provided to the Parliamentary Committee for Science and Technology by the NHS Confederation. They indicate a range of costs across different organisations within the NHS [EXHIBIT 8].

There is no doubt that the cost of fixing the millennium bug will be large.

<table>
<thead>
<tr>
<th>NHS organisations</th>
<th>Budget range (£000)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health authority (excl. primary care)</td>
<td>100-200</td>
</tr>
<tr>
<td>GP practice</td>
<td>2 - 22</td>
</tr>
<tr>
<td>Community trusts</td>
<td>30-150</td>
</tr>
<tr>
<td>Acute trusts</td>
<td>200-1,000</td>
</tr>
<tr>
<td>Teaching hospital</td>
<td>500-1,000</td>
</tr>
</tbody>
</table>

Source: NHS Confederation

99. Figures for local government as a whole are not yet available but the following information can help to provide an indication of the scale of the problem being faced by local authorities:

- one local authority has been quoted £30,000 to fix a non-compliant embedded system at a crematorium.

100. In a typical, large unitary council, there could be around 3,500 PCs in schools. The possible replacement cost could be high across the authority as a whole, but will also have a significant impact on individual school budgets. Given the scope of the problems that schools are likely to face, they may need assistance in managing year 2000 issues. The local education authority is ideally placed to provide such support.
101. Budgetary estimates for year 2000 projects are difficult to obtain. One complication is that the project is being funded from a variety of sources and budgets as follows:

• normal ongoing PC replacement;
• replacement of equipment from annual renewals budgets; and
• diversion of IT staff from other projects to deal with the year 2000 problem, funded from the annual IT budgets of central and departmental units.

102. Few of the authorities and trusts reviewed have made budgetary provision for the project as a whole. The cost is unlikely to be known until the project is well under way. Even then, new information will emerge, requiring adjustment to even the most thorough of plans.

103. The problem is exacerbated by the fact that while it is possible, when compiling an inventory for IT systems, to achieve almost 100 per cent coverage, this is not the case with embedded systems. Estimates for fixing computer hardware and software are beginning to emerge, but there is less information about the cost of replacing or fixing devices that contain embedded chips. In some instances, authorities and trusts cannot develop accurate estimates because information from some suppliers about the compliance of their product has not yet been received [BOX M].

104. Many predict that year 2000 costs will increase year on year [EXHIBIT 9, overleaf]. The later a project starts the more expensive the cost of solving any problems is likely to be. Using 1996 as a base, those organisations starting their projects in the first half of 1997 could face costs which are estimated to be 50 per cent higher than they would have been 12 months earlier.

105. Year 2000 staff contracts are proving to be expensive, and are becoming more so as resources become scarce and the end date draws closer. One local authority was quoted £750,000 for project management alone – this didn’t fix a single system! While recognising that the high demand for skills that are in short supply may mean that acquiring those skills will carry a premium, authorities and trusts should be wary of paying excessive rates. While tough negotiations may be required in some instances, responsible suppliers are more likely to adopt a reasonable approach, taking a long-term view of their business relationships.

Many predict that year 2000 costs will increase year on year.

BOX M

Developing a clear picture can be difficult
Information about compliance may not yet be readily available.

One NHS trust has four types of infusion pump in use throughout its hospitals. Year 2000 staff have still to receive confirmation from three manufacturers that their equipment is compliant and if not, what course of action is proposed. In the absence of such information, it is difficult to estimate what the cost will be. If replacement is necessary, the likely cost would be around £1,800 per pump. The hospital in question has up to 300 pumps on the wards and in specialist units.

Source : Audit Commission
EXHIBIT 9

Year 2000 costs escalation model

The later the project commences, the higher the costs are likely to be.

<table>
<thead>
<tr>
<th>Authority 1</th>
<th>Authority 2</th>
<th>Authority 3</th>
<th>Authority 4</th>
<th>Authority 5</th>
<th>Authority 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>1.25</td>
<td>1.50</td>
<td>1.88</td>
<td>2.25</td>
<td>2.81</td>
</tr>
</tbody>
</table>

Source: NCC

106. So what is the total cost likely to be? The truth is that, at present, no one really knows with any reasonable degree of certainty. We may not know until some time into the next century. The realities are that new problems are emerging and in those areas that are less critical, problems will not be fixed until after the year 2000.

107. This is not to say that budgets should not be established now. But they will need to contain some flexibility, where possible, in order to respond to sudden unforeseen requirements.

108. The position on funding in the NHS and local government, is that year 2000 costs are currently being met from existing resources which effectively means that they are being diverted from any new developments and initiatives. Additional initiatives with significant IT implications would place resources under even greater strain.

109. Chief executives have expressed some concern about the ability of authorities and trusts to tackle the year 2000 problems out of existing budgets. Further funds may be required if the pace of compliance activity and level of compliance is not to be seriously affected.
11. Conclusion and action

When the situation was manageable it was neglected.
Now that it is thoroughly out of hand, we apply, too late, the remedies which then might have effected a cure.

Winston Churchill 2nd May 1935

Authorities and trusts

110. Authorities and trusts are faced with a problem whose significance is due not so much to its technical nature as to its breadth. The millennium date problem can be fixed, but the pervasive nature of IT and embedded systems means that the scope of the problem in most organisations is very wide. Doing nothing is not an option. Action is required to stop things getting out of hand.

111. This paper has sought to emphasise the interdependencies that exist between all organisations in both the public and private sectors. It has sought to encourage an openness, by all, about preparations for achieving compliance or a state of readiness and the sharing of information for the common good. It provides a set of benchmarks against which organisations can measure their own progress and a situation report on progress to date.

112. At the time of writing, there are little more than 400 working days to the millennium. Year 2000 projects are entering an important phase when the achievement of targets will be even more critical. In this final phase of the project any slippage will necessarily result in a reappraisal of priorities, since the deadline is immovable.

113. There are a number of milestones and activities that are vital in the next phase of the project, up to the end of 1999 [EXHIBIT 10]. Authorities and trusts should concentrate on these tasks.

Doing nothing is not an option. Action is required to stop things getting out of hand.

EXHIBIT 10

Project milestones

Key stages in the next phase of the project.

<table>
<thead>
<tr>
<th>You should aim to have completed the following:</th>
<th>By this date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1998 Q2 Q3 Q4</td>
</tr>
<tr>
<td>Continue awareness</td>
<td></td>
</tr>
<tr>
<td>Review change control procedures</td>
<td></td>
</tr>
<tr>
<td>Update risk assessment</td>
<td></td>
</tr>
<tr>
<td>Prioritise actions</td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td></td>
</tr>
<tr>
<td>Remedial work</td>
<td></td>
</tr>
<tr>
<td>Re-testing</td>
<td></td>
</tr>
<tr>
<td>Contingency plans</td>
<td></td>
</tr>
<tr>
<td>Communications plan</td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
</tr>
</tbody>
</table>

Source: Audit Commission
Recommendations

The Audit Commission will:

1 continue to assess the preparedness of authorities and trusts and bring issues of concern to the attention of management;

2 assess what progress authorities and trusts are making as the millennium approaches;

3 publish update reports to this management paper;

4 share good practice advice;

5 encourage closer co-operation between authorities and trusts; and

6 keep under review the auditor's statement of responsibilities, as it may be affected by disclosures which authorities and trusts may be required to make in their accounts.

Government should:

7 note the likely levels of funding for year 2000 projects;

8 be alert to the consequences of legislation which has considerable implications for public sector IT within the next two years;

9 ensure that local government and the NHS are informed of progress with the Government's year 2000 project and those of major utilities;

10 take the lead in managing any interdependencies that cross international boundaries; and

11 consider how emergency plans should incorporate the year 2000 dimension.
The NHS Executive Year 2000 Programme, NHS Supplies Authority, NHS Estates, Medical Devices Agency, and equivalent organisations in Wales should:

12 act as the co-ordinating bodies for NHS organisations in respect of major IT supplies, medical devices, other equipment and supplies contracts;

13 evaluate responses from major suppliers;

14 apply pressure to obtain responses about compliance from major suppliers; and

15 distribute the results.

The Local Government Association should:

16 co-ordinate activities and facilitate the sharing of information for local authorities in England.

The Millennium Club in Wales should:

17 co-ordinate activities and facilitate the sharing of information for local authorities in Wales.
Appendix 1: Sample year 2000 inventory sheet

Here is an example of the sort of information which authorities and trusts have been collecting when compiling an inventory of systems and equipment.

YEAR 2000
INVENTORY SHEET

SPECIFICATION
1. System/equipment specification: __________________________
   Supplier __________________________
   Make __________________________
   Model/version number __________________________
   Serial number/licence number __________________________
   Supplier name and address __________________________

2. Is a replacement planned? Yes / No

3. If yes – when? __________________________

4. Is the system/equipment covered by a maintenance contract? Yes/No

5. When does it expire? __________________________

6. Is there a user group for the system? Yes / No

7. Name and address __________________________

IMPACT
8. If the system/equipment fails because of the year 2000 problem, what will the impact be on the organisation?
   catastrophic __________________________ q
   major __________________________ q
   moderate __________________________ q
   minor __________________________ q
   insignificant __________________________ q
**INTERFACES**

9. Does the system/equipment link to other systems/equipment? Yes / No
   Which systems/equipment? ______________________________
   ______________________________________________________
   ______________________________________________________
   ______________________________________________________
   ______________________________________________________

10. If the link is a computer interface, who provided and maintains it?
    _____________________________________________________
    _____________________________________________________
    _____________________________________________________
    _____________________________________________________

**YEAR 2000 COMPLIANCE STATUS**

11. Is the system/interface year 2000 compliant? Yes / No / Don't know

12. How do we know? User test / supplier test / supplier claim / other

13. If 'other' please specify: ________________________________
    ______________________________________________________
    ______________________________________________________
    ______________________________________________________
    ______________________________________________________

14. If the supplier has tested the system, are details of the test method and results available? Yes / No / Don't know

15. If the year 2000 compliance status is not known, when is the system first likely to display problems? ______________________________

16. If the system fails, is there a fallback plan? Yes / No

17. How long could we survive using this plan? __________________
Appendix 2: Members of the advisory group

Caroline Bramley
Cambridgeshire County Council

Stephen Dance
Arthur Andersen

Maynard Davies
Welsh Office

Ian Eddison
Action 2000

Adrienne Fresko
Audit Commissioner

Tim Jones
NHS Confederation

Alasdair Kemp
Institution of Electrical Engineers

Bryn Morris
Audit Commission

Ian Robertson
Local Government Management Board

Peter Rolfe
NHS Executive Year 2000 Programme

Allan Taylor
UNISON

Malcolm Teague
Plymouth NHS Trust

David Williams
Audit Commissioner

Paul A Williams
Arthur Andersen
The Audit Commission has produced a number of studies covering issues related to information technology and management in local government and the NHS. The following may be of interest to readers of this paper:

**Ghost in the Machine**  
*An Analysis of IT Fraud and Abuse*  
Update, 1998, 30 pages, 1862400563, £15  
(£10 to audited bodies)

**Worth More Than Money**  
*The Role of the Local Government Finance Director*  
Management Paper, 1998, 36 pages, 186240058X, £10

**Kiwi Experience**  
*VFM Messages from New Zealand*  
Occasional Paper, 1997, 36 pages, 186240013X, £8

**Representing the People**  
*The Role of Councillors*  
Management Paper, 1997, 40 pages, 1862400113, £7  
Pack of 10, 1862400245, £60

**Form follows Function**  
*Changing Management Structures in the NHS and Local Government*  
Management Paper, 1996, 40 pages, 186240003, £5.50

**Called to Account**  
*The Role of Audit Committees in Local Government*  
Management Paper, 1996, 28 pages, 0118864505, £6

**Improving Value for Money in Local Government**  
*A Compendium of Good Practice from Audit Commission Reports*  
Compendium, 1995, 62 pages, 0118864114, £8

**Taken on Board**  
*Corporate Governance in the NHS: Developing the Role of Non-executive Directors*  
Management Paper, 1995, 26 pages, 0118864303, £6

**Less Dangerous Liaisons**  
*Early Considerations for Making Mergers Work*  
Management Paper, 1995, 29 pages, 0118864408, £6

**High Risk/High Potential**  
*A Management Handbook on Information Technology in Local Government*  
Handbook, 1994, 96 pages, 0118861069, £11  
Executive Summary, 1994, 16 pages, 0118861263, £6

**Protecting the Public Purse 2**  
*Ensuring Probity in the NHS*  
National Report, 1994, 76 pages, 0118861468, £10

**Reaching the Peak?**  
*Getting Value for Money from Management Consultants*  
National Report, 1994, 46 pages, 0118861271, £6

**Protecting the Public Purse – Probity in the Public Sector**  
*Combating Fraud and Corruption in Local Government*  
National Report, 1993, 40 pages, 0118861182, £9

For a full catalogue of Audit Commission publications, please contact the Communications Department, Audit Commission, 1 Vincent Square, London SW1P 2PN, Telephone 0171 828 1212.

To order Audit Commission publications, please telephone 0800 502030, or write to Bookpoint Ltd, 39 Milton Park, Abingdon, Oxon OX14 4TD
The year 2000 poses problems for all organisations that rely upon computers and other equipment which contains microchips. For the NHS and local government there could be serious implications for public health and safety. Preparation for the new millennium is a major management challenge. Organisations that delay taking action increase the risk that key services will fail.

The Audit Commission has written this paper to help members, non-executive directors and chief officers in local government and the NHS to minimise the risk of serious disruption.