![NAO logo] NATIONAL AUDIT OFFICE

The Millennium Threat: Are We Ready?

JUST AHEAD Y2K

Contents

Executive summary

What is the problem and how has it arisen?

1   The Year 2000 problem or the "millennium threat" arises because in the past many computer programmers referred to years by their last two digits rather than by all four ("99" instead of "1999"). As a consequence some computers and other electronic equipment processing dates may assume that "00" means "1900" rather than "2000" and may produce meaningless information or fail completely. In addition, some systems do not recognise 29 February 2000, which is a leap day under the Gregorian calendar. This Report:

- updates progress on the action taken by the Government to safeguard essential services in the United Kingdom over the millennium period;

- updates Year 2000 progress in central Government Departments and Agencies;

- examines emergency planning arrangements in the UK and how these have been enhanced to cater for the effects of the millennium;

- examines how Year 2000 failures abroad will affect the UK and the advice provided for travellers abroad and businesses with offices overseas.

2   There are few areas of modern life that are not touched by information technology (IT). The millennium threat is a business wide problem that affects everyone: even if internal systems are Year 2000 compliant, activity may still be disrupted if the systems of suppliers or customers fail. With the end of 1999 so close, there is now little more that can be done to put systems right, and attention is now on how to address the remaining risks of failure and ensure that business can continue by alternative means if necessary. The focus is therefore on devising continuity plans, testing them, and on preparing detailed millennium operating regimes.

Who is responsible for taking action to overcome the millennium threat?

3 The Government's objective is to "ensure no material disruption to the essential public services of the United Kingdom". It established a Ministerial Group to co-ordinate action across Government and the whole of the national infrastructure. Action 2000, a company limited by guarantee and sponsored by the Government, works with the Cabinet Office, who support the Ministerial Group and have the lead role in co-ordinating action and monitoring progress. But primary responsibility for action to overcome the threat rests with individuals, individual companies, Government Departments, statutory Regulators, and other public sector bodies.

What are essential services and how has their millennium readiness been assessed?

4 A wide range of private and public sector organisations delivers essential services, and many depend on each other for continuity. In March 1998, the Cabinet Office commissioned a review to identify and map essential services of the United Kingdom. The result was the 58 high level processes (in 25 sectors) listed at Appendix 3.

5 For each process, Action 2000 identified "responsible bodies" to commission, monitor, and publish the results of an independent assessment programme, undertaken to a common set of standards. This included a "traffic light" rating system to indicate progress towards millennium readiness (shown at Figure 6 on page 16). The scope of these assessments has expanded as the year-end has drawn closer, and the latest results include an assessment of business continuity plans and millennium operating regimes.

What are the results of the assessments, and what are the remaining risks to "no material disruption"?

6 The results announced on 21 October show a further substantial improvement in the overall picture with only two of the 25 sectors in Great Britain with a partly amber rating (some risk of material disruption, but rectification plan in place) and a further three with elements with a very small part amber rating which do not affect the overall blue rating for the sector (shown in Figure 1). This is a major achievement, and it is clear that for the key infrastructure processes the risk of major failures arising as a result of the millennium threat is now low.

What about businesses not assessed as part of the essential services of the UK?

7   Outside of the essential services of the UK national infrastructure, Action 2000 surveys of businesses conducted in August and reported in September show that progress continues and in larger companies is good. However, more than one quarter of businesses with 10 to 249 employees have an identifiable risk but are not taking the full range of steps to address Year 2000 issues. In addition, progress on continuity planning is not as far advanced as might be expected.

Will central Government Departments and Agencies be ready?

8   Good progress continues, but so does slippage. In the September 1999 review, there are seven bodies reporting completion dates for business critical systems of October 1999 or later. And five of these bodies did not expect to have complete and tested business continuity plans and millennium operating regimes by the end of September.

9   The picture for non-critical systems is worse, with 20 bodies reporting completion dates after September 1999. Failures here may well cause inconvenience and additional work as "workarounds" are implemented.

10   Although progress on business continuity planning and millennium operating regimes has been good overall, two thirds of continuity plans were not expected to be tested by the end of September.

Are emergency planning arrangements robust, tested, and have they been adequately enhanced to deal with the millennium?

11   The Home Office have the primary responsibility for emergency planning in the United Kingdom. There are well developed and tested plans for dealing with emergencies, based on a local response, which escalates to assistance from adjacent areas and central Government if necessary. The millennium threat and millennium celebratory events add to the potential for problems because local mutual assistance arrangements may be limited by problems arising elsewhere.

12   Emergency planning arrangements are tested through routine exercises. In many cases, the normal arrangements have been enhanced with millennium specific preparations, and by increasing the normal level of activity. The Home Office have issued best practice guidance. Exercises to test arrangements, up to and including ministerial level, have been held.

13 The Government will be monitoring events both nationally and internationally through a Government wide millennium operating regime, providing a centrally co-ordinated information service on the national picture. These arrangements were also tested at the end of October 1999.

What is the overseas position?

14 Year 2000 problems overseas could cause problems in the UK if they disrupt supply chains. International elements of services delivered and consumed in the UK (for example, food supply and distribution) are included in the colour coding because they are assessed as part of the normal supply chain risk, and the risks are addressed in business continuity plans. However, this does not extend to the overseas elements of services delivered and consumed outside the UK (for example, postal services to an overseas location) because of the difficulty in gathering accurate and reliable information from overseas. The Foreign and Commonwealth Office (FCO), the Department of Trade and Industry, Action 2000, responsible bodies and service delivery organisations have worked with some international bodies to appraise key aspects of the international supply chain. But overall, in comparison with the UK, we have less reliable information about readiness.

15 For travellers abroad, and British businesses, the Foreign and Commonwealth Office have published a series of country statements and Year 2000 travel advice notices on their Internet web site compiled from a range of public and other sources, providing information on their millennium preparedness. In addition, other countries have undertaken similar reviews and there are many other web sites providing Year 2000 information on individual countries. However, it is difficult for the FCO to verify the completeness and accuracy of these statements, and the information contained may quickly become out of date despite the FCO's best efforts to keep the information current. Businesses and travellers seeking advice therefore need to trawl a wide range of information sources.

What are the main areas of concern now?

16 Figure 1 summarises the remaining areas of concern.

Figure 1

Remaining areas of concern

Status and comments

National Infrastructure Sectors	Position at 21 October 1999		
	Blue	**Amber**	
Financial Institutions	98%	2%	7 medium impact firms amber. 100 per cent blue expected by 12 November 1999
Gas (Domestic Shippers and Suppliers)	99.7%	0.3%	100 per cent blue expected by 31 October 1999. (York Gas that trades only in Yorkshire)
Transport Services to the Scottish Islands	98%	2%	CalMac expected to be 100 per cent by 22 October 1999 (and achieved) Loganair currently being independently assessed.
Rail Transport (Light Railways)			Manchester Metrolink not yet independently assessed

Central Departments and Agencies	Position forecast at 30 September 1999
Foreign and Commonwealth Office	Business critical IT and telecommunications systems completion in October.
	Business continuity plan not completed or tested. Forecast to be completed in October.
Defence Procurement Agency	Business critical IT systems completion in October.
	Business critical embedded and telecommunications systems completion in October.
	Business continuity plan not competed or tested.
	Millennium operating regime incomplete.
Ministry of Defence (Centre)	Business critical IT systems completion in October.
	Business critical embedded and telecommunications systems completion in December.
Planning Inspectorate	Business critical IT systems completion in November.
	Business continuity plan not complete or tested.
	Millennium operating regime not complete.
The Rent Service	Business critical embedded systems completion in November.
	Business continuity plan not tested.
	Millennium operating regime not complete.
Royal Air Force	Business critical IT and embedded systems completion in October.
Serious Fraud Office	Business critical IT systems completion in October.
	Business continuity plan not tested.
	Millennium operating regime not complete.

Businesses outside the national infrastructure assessment arrangements	Position reported on 28 September 1999 (based on research in August 1999)
Businesses with 10-249 employees	27 per cent have an identifiable risk but are not taking the full range of steps to address Year 2000 issues.
	Continuity planning not as advanced as expected.
Overseas	Completeness and accuracy of information available on millennium readiness of other countries.

Have citizens and businesses been kept informed?

17   Action 2000 and Government have undertaken a series of publicity campaigns to keep both citizens and businesses informed, advertising in the national press, and through the issue of booklets to households and businesses. Press conferences have been held to present key messages. The Action 2000 Internet web site (http://www.bug2000.co.uk) provides comprehensive coverage of their work, and the results of national infrastructure programme assessments and research surveys of progress in UK businesses.

18   Progress in central Government Departments and Agencies has been regularly reported to Parliament, and has attracted some media interest. The detailed progress reports from Departments and Agencies are published on the Internet (http://www.citu.gov.uk/y2000).

19   The Foreign and Commonwealth Office "country statements" and advice for travellers abroad are published on the Internet (http://www.fco.gov.uk), and have also attracted media interest.

What must happen now?

20   The UK has undertaken a significant programme of work to counter the millennium threat. Although the risks of material disruption to essential services are diminishing, there is still work to be done. With 51 days to go to the millennium, the focus of attention must be on continuing to assess the remaining risks to "no material disruption" and keeping business continuity plans to address them up to date. This applies to all organisations – the key providers of the national infrastructure, central Government Departments and Agencies, and all businesses of what ever size outside the scope of the national infrastructure assessments. In addition, all organisations must consider how operations over the millennium period itself will need to differ from normal, not only assessing how they will monitor electronic systems, but also how the millennium will affect demands on the organisation, and so on. In the few remaining weeks considering and devising a millennium operating regime is therefore essential.

21   In addition, beyond the millennium itself, some systems may not recognise 29 February 2000 as a leap day, and continuity plans and millennium operating regimes must cover this date as well.

22   We therefore recommend that all organisations:

■ prepare and review business continuity plans:

❑ continue to review risks to business continuity as more information about millennium preparedness in other organisations and sectors becomes available;

❑ prepare and revise business continuity plans accordingly;

❑ test them through exercises involving key staff;

❑ keep all staff informed of this work, and what will be required of them over the millennium period;

■ prepare and review millennium operating regimes:

❑ continue to make detailed preparations for operations over the millennium period and other key dates covering critical aspects of business activity;

❑ keep staff informed of the action they will be expected to take as part of the regime;

■ keep the public, businesses, customers, and suppliers informed of all actions taken to enhance millennium readiness and reduce risk of disruption to normal services so that confidence is maintained. In particular:

❑ results of continuing assessments and monitoring of millennium preparedness;

❑ business continuity plans;

❑ millennium operating regimes;

❑ emergency planning arrangements;

❑ developments overseas.

Part 1: Background

What is the problem and how has it arisen?

1.1   The Year 2000 problem or the millennium threat or millennium bug has arisen because in the past computers and other electronic systems referred to years by their last two digits rather than all four ("99" instead of "1999"). As a result, many computer systems and other electronic equipment cannot tell the years 2000 and 1900 apart and may produce meaningless or incorrect information, or may fail completely, when trying to deal with dates after the century change. In addition, 29 February 2000 is a leap day under the Gregorian calendar. For some systems, particularly equipment containing embedded chips, testing has revealed that they do not recognise this date.

1.2   This problem potentially affects everyone, and work to counter the threat over the last three years or so has made organisations appreciate that it is a business wide problem and not just an information technology problem. The millennium bug can affect equipment not traditionally thought of as computers, such as security systems and telephones (often called embedded systems). In addition, almost all organisations are dependent on others for supplies of materials and utility services. Even if an organisation's own systems are millennium compliant it has to consider how its suppliers and customers are addressing the threat so that business can continue.

1.3   With around seven weeks to go before the millennium, there is little more that can be done to put right computers or equipment. The focus now is on ensuring that rigorous tested continuity plans and effective millennium operating regimes are put in place.

What are the dates when failures might arise, and why?

Figure 2

The millennium bug is generally thought to "strike" on 1 January 2000, but there are various dates on which failures or incorrect information might arise when used in computer applications or systems. The key dates are:

9 September 1999 – ninth day of the ninth month of year ninety-nine. In some older computer programs "9999" was used to indicate "end of file" or "stop program".

1 January 2000 – the 99 to 00 roll over problem described in paragraph 1.1.

29 February 2000 – the leap year day in 2000 under the Gregorian calendar. Some applications do not recognise 2000 as a leap year (1900 was not a leap year), and rectification is required to ensure correct data is produced.

1 January 2001 – the first year roll over in the new millennium.

29 February 2004 – the first leap year day after 2000, to ensure leap year recognition works beyond 2000.

Despite previous speculation, the IT industry expected few "9999" failures and none were reported in the media, although this is not to say that failures did not arise.

On 23 September, Mrs Margaret Beckett, Leader of the House of Commons, confirmed in a letter to all MPs that "9999" had no adverse impact on Departments' and Agencies', systems.

The Global Positioning System

Figure 3

Although not specifically a millennium failure, the Global Positioning System (GPS) provided a further example of possible failures that might arise due to roll over of data.

The GPS is a world-wide satellite system which allows navigators to pinpoint their position anywhere in the world. The GPS started life on 6 January 1980 and keeps track of time by counting the number of weeks, but it was programmed to recognise a maximum number of 1024 weeks. On 21 August 1999, the 1025th week, the counter rolled over to zero, and receiving equipment that had not been programmed to cope either failed completely or provided inaccurate data.

No business critical failures were reported, indicating that older GPS equipment had either been replaced or re-programmed to cope with the roll over, or alternative navigation aids were used to maintain continuity. However, there were some reports of failures of older devices in cars in Japan, where the GPS is more widely used for road navigation.

Implementing a Y2K upgrade: London Electricity "Powerkey" pre-payment customers

In early August 1999, London Electricity issued new "Powerkeys" containing an upgrade to make them Year 2000 compliant. The new keys contained upgraded software and details of the customer's latest payment, but the upgrade did not always credit the meter for the electricity paid for. In some cases it completely corrupted the meter leaving the consumer without an electricity supply.

London Electricity took quick action to deploy repair teams and brief consumers but some 2000 customers were left without electricity for a few days (www.london-electricity.co.uk).

Who is responsible for taking action to overcome the millennium threat?

1.4 The millennium threat affects everyone – citizens, businesses in the private sector, and the public sector. Action to overcome the threat is the responsibility of individuals, individual companies, Government Departments, Agencies, statutory Regulators, and other public sector bodies.

1.5 In the United Kingdom, the Department of Trade and Industry took the lead in raising awareness of the problem. A key development was the Prime Minister's announcement in March 1998 that the Government's objective was to "ensure no material disruption to the essential public services of the United Kingdom on which the public rely". At the same time, the Government established a Ministerial Group to co-ordinate action across Government and the whole of the national infrastructure. A Year 2000 team was created in the Cabinet Office, and with Action 2000, a company limited by guarantee and sponsored by the Government, started a programme of work to ensure "no material disruption" and sustain public confidence that essential services would continue to operate as normal over the millennium period.

1.6 Action 2000 established the National Infrastructure Forum to promote information exchange, the sharing of best practice, and independent assessment to help meet the Government's objective. Membership has steadily grown so that it currently comprises around 350 organisations from 25 sectors, public, private and regulated, who deliver essential services in the UK. Within the Forum, a Steering Group works on policy matters and an Advisory Group exercises a critical review of Action 2000 activities.

1.7 The Cabinet Office have the lead role in monitoring progress in central Government Departments and Agencies. Within the central Government sector, responsibility for action to counter the millennium threat falls to individual Departments and Agencies. The Foreign and Commonwealth Office has led on the action being taken to inform the public and industry of the preparedness of other countries and to assess and address the risks to British interests from failures abroad.

1.8 The relationship between these bodies is shown at Figure 5. A chronology of Year 2000 dates in achieving millennium readiness in the United Kingdom is at Appendix 1.

Government Year 2000 framework

Figure 5

Prime Minister

Leader of the House
Chair of Ministerial Group

Ministerial Group
Co-ordinate action across Government and the national infrastructure, ensure no material disruption

Year 2000 Team in the Cabinet Office
Support Ministerial Group, monitoring progress across Government

Action 2000
Support to businesses, orchestrate independent assessment, help sustain public confidence

Central Departments and Agencies
Ensure their own continuity of service

Department of Trade and Industry
Alert British industry

Foreign and Commonwealth Office
Provide advice on preparedness overseas, briefing industry on overseas scene

National Infrastructure Forum
Chaired by Action 2000, promote independent assessment and information exchange

Source: NAO

Earlier Reports by the Comptroller and Auditor General and the Committee of Public Accounts

1.9   This Report follows up our four earlier Reports specifically on the Year 2000 problem:

- "Managing the Millennium Threat" (HC 3, Session 1997-98);

- "Managing the Millennium Threat II" (HC 724, Session 1997-98);

- "How the Utility Regulators are Addressing the Year 2000 Problem in the Utilities" (HC 222, Session 1998-99);

- "The Millennium Threat: 221 Days and Counting" (HC 436, Session 1998-99).

1.10   We have also reported on specific issues and sectors as part of our wider work (for example, the National Health Service Summarised Accounts in England, Scotland and Wales). A full list of earlier reports by the Comptroller and Auditor General and the Committee of Public Accounts is at Appendix 2.

1.11   On the basis of our report "The Millennium Threat: 221 Days and Counting" (HC 436, Session 1998-99), the Committee of Public Accounts took evidence from the Cabinet Office and Action 2000 on progress in tackling the millennium threat for the national infrastructure, and central Government Departments and Agencies. In their subsequent report ("The Millennium Threat", 36th Report 1998-99 (July 1999)), the Committee recommended:

- on progress made:

  - that although the national infrastructure programme was comprehensive and to be welcomed, guarantees of no material disruption could not be given, that progress in some key sectors was disappointing, and that this made it essential that properly scoped, good quality and tested business continuity plans were in place;

□ that delays in completing millennium compliance work were exacerbated by poor progress in preparing business continuity plans, and that the Cabinet Office should continue to exert strong pressure on all central Government and other public bodies to complete both compliance and continuity planning work;

■ on keeping citizens and businesses informed:

□ that information should be cascaded throughout the country so that people knew how their local services were coping;

□ that those bodies where there was still a risk of material disruption should be named and that the public deserved to be told about the millennium readiness of all bodies;

□ that the utility Regulators should consider what more they and the utility companies could do to ensure that customers were properly informed about preparations being made by their local utility companies;

□ that to help travellers abroad and businesses with overseas offices or suppliers, the Foreign and Commonwealth Office should make country specific information available as soon as possible.

Scope of this Report

1.12 This Report looks at:

■ progress in tackling the millennium threat for essential services in Great Britain (Part 2), and across central Government Departments and Agencies (Part 3);

■ how emergency planning arrangements have been enhanced to take account of the millennium threat and millennium celebratory events (Part 4);

■ progress in identifying the likelihood and effect of millennium failures overseas on the UK infrastructure, businesses with overseas offices and travellers abroad (Part 5).

1.13 This Report excludes the position in Northern Ireland, which is outside the scope of the work of the National Audit Office.

1.14 In parallel with this Report, we have produced separate Reports on Scotland and Wales, focusing specifically on those elements of the national infrastructure provided locally, the readiness of the Scottish Executive and the National Assembly for Wales, and emergency planning. We have also produced a further Report to update the work of the Utility Regulators in addressing the Year 2000 problem in the utilities.

How have we conducted this investigation?

1.15 Our examination has focused mainly on progress reports and surveys by Action 2000, the Cabinet Office and other public sector bodies, and information on the Internet on the readiness of other countries.

1.16 We plan a further Report in the Spring of 2000 to look at any problems that emerged over the millennium period, how well they were handled, what further work needs to be done, and lessons learnt from work to counter the millennium threat.

Part 2: The UK National Infrastructure

What are essential services in the United Kingdom?

2.1   Within the United Kingdom a wide range of organisations deliver essential services. These can be private sector companies, organisations regulated by the Government, central and local Government bodies and wider public sector bodies. These essential services are often dependent on each other. In some cases dependencies are obvious – virtually all services depend on electricity and telecommunications – but in others dependencies are less clear. For example, food supply depends on supply of raw ingredients, production and processing utilising a wide range of services, packaging, fuel for distribution to wholesalers and retailers, and in many cases, electricity for freezers for selling to the customer.

2.2   In March 1998, the Cabinet Office commissioned Ernst and Young to identify and map the essential services of the United Kingdom to show the flows and connections between them. The result was definition of 58 high level processes with around 1000 lower level processes, within 25 sectors. The full report is available on the Internet at http://www.citu.gov.uk/y2000.htm . The high level processes within sectors are listed at Appendix 3.

Assessing millennium readiness

2.3   The millennium readiness of each sector and process has been assessed through a programme of independent assessment, which started in October 1998. The aim of the programme has been to ensure that each service supplier has carried out a robust programme of work to counter the millennium threat, and that claims of readiness are credible.

2.4   The assessments are undertaken to a common set of standards published by Action 2000. To ensure a consistent approach and enable comparisons between sectors Action 2000 also introduced a traffic light code to chart the progress towards achieving "no material disruption" in essential services over the millennium period (Figure 6).

Independent assessment programme: status indicator colour codes

Figure 6

Colour code	Description
⚪	Unable to form assessment with the present level of information.
🔴	The assessment indicates that there is a severe risk of material disruption to infrastructure processes and that timely rectification may not be possible.
🟠	The assessment indicates that there is some risk of material disruption to infrastructure processes, but that there is an agreed containment plan to rectify shortcomings.
🔵	The assessment has not indicated any risks of material disruption to the infrastructure processes.

Source: Action 2000

What factors were taken into account when assessing millennium readiness?

2.5   The Year 2000 programmes of individual organisations have expanded over time, as the millennium drew nearer, to take account of an increasing range of factors:

- own systems – working on inventories, compliance assessment, rectification, and testing (with work on IT systems generally starting before that on embedded systems);

- supply chain – identifying risks posed by disruption from suppliers or customers and how to reduce or eliminate them;

- wider infrastructure – considering the likelihood and potential impact of disruption arising from failures in the wider infrastructure;

- demand and behaviour – identifying potential changes in demand for services and the impact of abnormal behaviour caused by the millennium threat or millennium events;

- continuity planning – developing and maintaining plans to maintain business continuity so as to counter residual risk as the factors above change;

■ millennium operating regime – specifying arrangements for operations over the millennium period, where these differ from normal. These include both a planned element and a contingency element to deal with unforeseen events.

2.6 For individual sectors and processes within the national infrastructure, some of these factors have been added since the programme of independent assessment started in October 1998. More information has become available, and the results of the assessment programme itself have been published and provided confidence of continuity in various sectors. In parallel, as the assessment programme has continued, more of these factors have been taken into account in reaching a view on the traffic light coding of processes and sectors, with the coding representing the assessment of the risk of material disruption at a given point in time. However, the final assessments announced from October 1999 onwards, and subsequent monitoring activity encompass all of the components listed in paragraph 2.5. Figure 7 illustrates how components of assessments have changed over time.

Factors considered in independent assessments

Figure 7

Information Systems

Embedded Systems

Supply Chain

Wider Infrastructure

Demand/behaviour

Continuity Planning

Millennium Operating Regimes

Initial assessments

Latest assessments and monitoring

Assessments reported in:

Jan 99   Apr 99   Jul 99   Oct 99   Dec 99
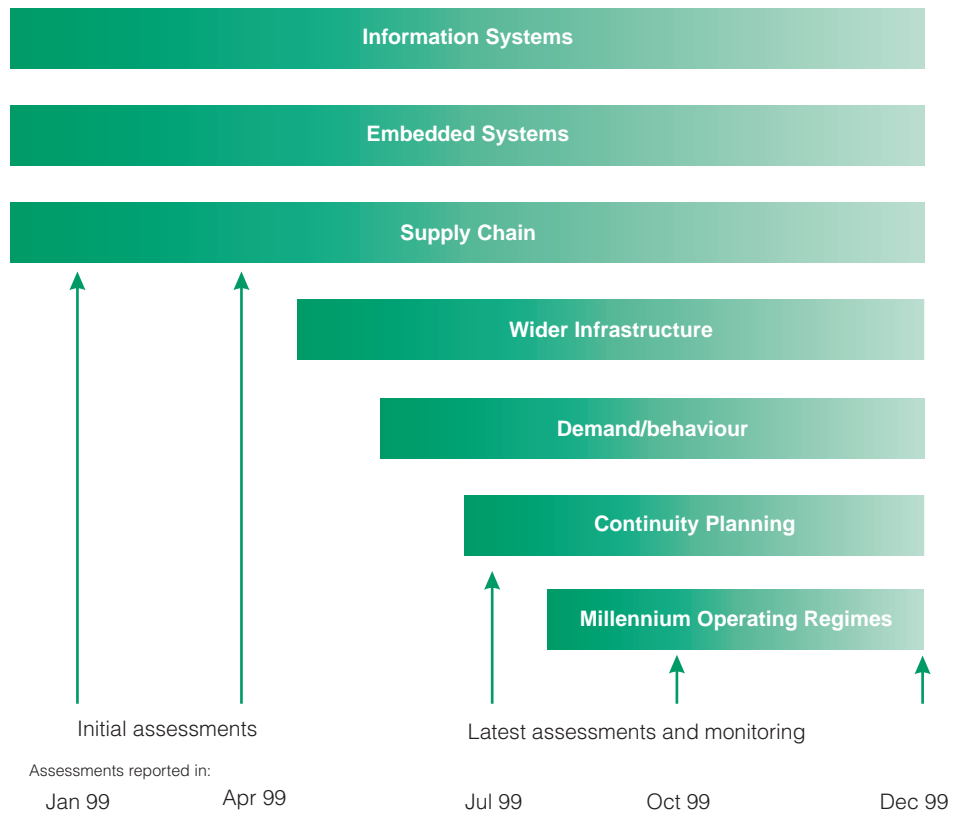
Source: Action 2000 and National Audit Office

What are the results of the independent assessments?

2.7   The independent assessment programme was initially managed in three tranches, with those sectors with most inter dependencies, such as utilities, assessed first. Assessments for all sectors were available in July 1999. Results of the latest position announced at the National Infrastructure Forum meeting on 21 October are summarised at Figure 8. Appendix 4 shows the results in more detail, with the results of earlier announcements for tracking progress and comparison. For most sectors, assessment results are also available by process and by organisation and details are on the Action 2000 Internet web site (http://www.bug2000.co.uk)

Results of independent assessments reported on 21 October 1999

Figure 8

Electricity   Water and Sewage   Essential Food and Groceries
Telecommunications   Air Transport   Road Transport
Rail Transport   Hospitals and Healthcare Fire Services
Sea Transport   Broadcasting   Local Government
Police   Post and Parcels   Weather Forecasting
Sea Rescue   Flood Defence   Criminal Justice
Welfare Payments   Bus Transport   Newspapers
Tax Collection   Fuel Supplies

Financial Services

Financial processes   **100%**

Financial Institutions   **98%**   **2%**   Projected to be 100% blue by 12 November 1999.

Gas

Transportation and safety   **100%**

Domestic Shippers
 and Suppliers   **99.7%**   **0.3%**   Projected to be 100% blue by 31 October 1999.

Transport Services to the Scottish Islands

Sea Transport (CalMac)   **98%**   **2%**   Projected to be 100% blue by 22 October 1999 (and acheived).

Air Transport (Loganair) currently being independently assessed, results expected in November.

Light Railways - Manchester Metrolink not yet independently assessed, results expected in November.

2.8 It should be noted that the international elements of services delivered and consumed in the UK are included in the colour coding because they are assessed as part of the normal supply chain risk. Foreign elements of services delivered and consumed outside the UK are not included. Further information on the international picture is at Part 5 of this Report. A case study of the Year 2000 programme at Hyder – providers of utilities in Wales – is at Figure 9a, and of independent assessment at the Met Office is at Figure 9b.

What are the remaining risks to no material disruption of essential services?

2.9 The results show a very much improved picture, with 23 sectors having a 100 per cent blue rating (no indicated risks of material disruption) and only two sectors with part amber ratings (some risk of material disruption but agreed rectification and containment plan in place). A further three sectors have very small elements with part amber ratings that do not affect the overall blue rating of the sector. No sectors are rated red or partly red.

2.10 Those sectors with part amber ratings expect to achieve a blue rating shortly, so that all key processes in the UK national infrastructure will be rated blue by November 1999.

Case Study: Year 2000 programme at Hyder - providers of utilities in Wales

Figure 9a

Background to Hyder's Year 2000 Programme

Hyder are an integrated multi-utility company with a core market for services in Wales. They hold franchises for water supply and wastewater services serving some 3 million people, through Dwr Cymru Welsh Water. Hyder also provide electricity and gas supplies through the business brand of SWALEC.

A large proportion of Hyder's utility operations and networks are controlled by electronic equipment. Not all are date sensitive but many are critical to the business and the ability to maintain continuity of service to customers. For example, on most water treatment works electronic equipment is used to control operations, monitor water quality, provide accurate doses of chemicals for treatment purposes and to provide continuous feedback of information to the network control centre. Hyder's electricity distribution network is controlled in a similar way.

Large mainframe computers running software and applications for both operational and management purposes underpin this infrastructure. Hyder also have thousands of personal computers and hundreds of smaller software programs many of which interface via the group's telecommunications network. Hyder has a complex chain of suppliers and service providers all of whom are themselves reliant on computer based systems.

Overall Year 2000 Programme Status

Hyder started their Year 2000 programme in the early part of 1997. The programme is sponsored at Executive Director level and throughout all work has been closely monitored by the Board of Directors.

Case Study: Year 2000
programme at Hyder -
providers of utilities
in Wales *continued*

Figure 9a

Hyder believe they are ready for the millennium. Across the group, they have assessed systems and equipment and have introduced a programme of work aimed at minimising the risks that computer systems and operational equipment might fail or function incorrectly as a result of the Year 2000 date change. Their Year 2000 programme has cost £16 million, covering all water and sewerage operations, electricity distribution and supply systems, customer services applications, buildings, IT support services and systems and the compliance of key suppliers. Hyder have adopted the British Standards Institute definition of Year 2000 conformity (DISC. PD 2000-1:1998) for this work.

Independent Assessment and Auditing

Hyder's internal auditing programme commenced at the outset of the project in 1997. A rolling programme covers all aspects of the project. The internal audit programme was designed to ensure compliance with centrally defined Year 2000 project management procedures and to monitor that key project deliverables were being successfully met. Technical methodologies for testing IT and embedded systems have also been audited by independent consultants to ensure consistency with best practice. Hyder engaged Ernst & Young to conduct a series of independent external audits.

Hyder have also completed a comprehensive review of their supply and dependency chain to ensure that key suppliers have made appropriate steps to address the Year 2000 issue and that any residual risks are known and understood.

The utility regulators (OFWAT and OFGEM) are responsible for ensuring that utility companies make effective Year 2000 preparations and the NAO Reports "How the Utility Regulators are Addressing the Year 2000 Problem in the Utilities" (HC 222, Session 1998-99) and "The Year 2000 Problem in Utilities: Update Report:", (HC 843, Session 1998-99) provide further information.

As part of Action 2000's national infrastructure programme the utility regulators (in the role of responsible body) have engaged independent consultants to undertake end to end Year 2000 assessments for individual companies, using Action 2000's traffic light classification for Year 2000 readiness. Hyder's gas, electricity and water businesses are now all classified as blue status, meaning that the assessment has not identified any risks of material disruption arising from the Year 2000 issue. The findings of these independent assessments form an important part of Hyder's "business as usual" Year 2000 message and provide an additional level of confidence to customers.

Case Study: Year 2000 programme at Hyder - providers of utilities in Wales *continued*

Figure 9a

Communication and Awareness Initiatives:

A further element of Hyder's Year 2000 programme is keeping customers and other external organisations fully informed of their preparations. Year 2000 enquiries, mainly from larger organisations, reached a peak in July 1999. To ensure an efficient response, a range of standard Year 2000 documentation has been produced, including a brochure, a project methodology statement and individual fact / status sheets covering electricity (gas) and water services.

This direct method of information disclosure has been supported by a variety of other communication initiatives designed to increase the general awareness of the Year 2000 issue within specific sectors of the Welsh economy including :

■ supporting the Government's Action 2000 mentoring scheme by sponsoring a series of "awareness" seminars throughout Wales;

■ chairing the Water UK industry-wide millennium bug group designed to share information and technical resources with others and formulating best practice guidelines

■ convening Year 2000 seminars targeted specifically at Health Trusts, Police and Fire services to communicate Hyder's Year 2000 preparations and establish an initial dialogue and points of contact;

■ in conjunction with the Environment Agency, Wales, Hyder is undertaking a major awareness and risk assessment initiative targeted at trading organisations with the potential to pollute water courses and / or sewers. The aim was to ensure that key organisations were aware of the Year 2000 issue and had taken appropriate steps to mitigate any potential impacts. The initiative consisted of seminars with a follow up mailing of self help checklists to organisations.

Contingency Planning and Millennium Operating Regime

In addition to their work to minimise the potential effects of the millennium bug, Hyder have also put contingency plans in place.

Hyder's energy and water businesses already have incident management and disaster recovery plans which are fully documented and routinely tested. As part of the Year 2000 programme, these plans have been reviewed and where necessary supplemented to ensure that risks are further minimised and that the businesses are in an optimum operational state over the New Year period.

Hyder's millennium operating regime (MOR) co-ordinates Year 2000 specific contingency plans with existing emergency and business continuity plans. The MOR defines how Hyder's business will operate over the New Year period, how and where staff will be deployed, the procedures for situation reporting and the management structure for incident response and containment.

These plans have been developed in liaison with, and are integrated with, emergency response plans being prepared by emergency services in Wales. At the higher level, millennium operating plans are being co-ordinated via a Year 2000 forum established by the Welsh Assembly.

Case Study: Independent Assessment at the Met. Office

Figure 9b

Introduction

The Met. Office provide the majority of weather forecasting services to the UK and, as the national meteorological authority, are responsible for the collection of meteorological data nationally and from overseas. Many sectors of national infrastructure depend on meteorological services, especially forecasts for the safe and effective continuance of many of their key services to the UK economy.

The Met. Office are recognised by the World Meteorological Organisation (WMO), an agency of the United Nations, and their Chief Executive is the Permanent Representative with WMO. They have responsibilities under national and international agreements for the collection and provision of meteorological information and forecasts.

Scope and Depth of Assessment

The National Audit Office were commissioned to be the Independent Assessor of The Met. Office's Y2K programme and the meteorological services they provide to the national infrastructure. The National Audit Office fieldwork for this assessment took place in two phases in May 1999 and September 1999. The assessment included all of the Met. Office business processes that are required to deliver the services identified in the Action 2000 national infrastructure model.

Assessment Process

The work consisted of:

- review of the scope of the Year 2000 programme;
- evaluation of The Met. Office Year 2000 management processes;
- review of standards set by the central Year 2000 team;
- examination of evidence that the interim and final certification process was working;
- observation of the clean management audit and risk review processes;
- review of the testing and business continuity planning processes;
- interviews of staff managing key projects.

An internal Met. Office certification scheme involves a formal review of the project documentation to ensure compliance with The Met. Office standards. Review meetings, chaired by the Year 2000 Programme Manager or his deputy, result either in a certificate of compliance or an exception report and list of actions. Interim certification was completed in December 1998. Final certification was completed in September 1999. Risk reviews, testing results and clean management audit reports fed into the final certification process.

The certification process has delivered:

Assurance of continuing Year 2000 compliance: one of the major risks associated with the Year 2000 compliance management process is that systems and procedures may be examined, possibly modified to make them Year 2000 compliant and then be allowed to become non-compliant again by the application of changes which re-introduce non-compliance. The Certification Process ensures that not only is there documented evidence that the systems and procedures have been rendered Year 2000 compliant, but also that they remain so. The Clean Management Strategy sets out the technical approach towards ensuring that changes are managed correctly, the Certification Process is the mechanism by which the technical approach is monitored.

Case Study: Independent Assessment at the Met. Office *continued*

Figure 9b

Reduction of risks associated with unexpected Year 2000 problems: although Compliance Projects have sought to ensure that all Year 2000 problems are identified and corrected prior to the Year 2000, unexpected problems may arise. It is important that contingency plans are put in place to ensure that such problems can be managed effectively and their impact minimised. The award of Compliance Certificates addresses not only the elimination of Year 2000 problems but also the way in which contingency plans have been set in place.

Provision of a project progress monitoring mechanism: at the Project 2000 Programme management level there is a need for the Programme Board to be able to monitor the progress of the Compliance Projects. The Certification Process provides them with an independent, certificated assurance of a Compliance Project's Year 2000 compliance work as well as a certificated assurance that the Compliance Project has completed all testing, has an adequate recovery plan and is applying an effective Change Control and Change Management regime.

The Met. Office Year 2000 certification scheme has some well-defined milestones:

Scope Certification: a sub-set of the System Inventory is called the "Compliance Library" which groups systems together, defines compliance project responsibilities, and includes a snapshot of their status and forms the basis for work on remediation.

Interim Certification: interim certification included a review of the Compliance Project inventory, risk register, test results and clean management plan.

Clean Management Review: clean management ensures that tested configuration items are not rendered non-compliant by subsequent changes.

Risk Review: risk review meetings held prior to each final certification review to assess the residual risk to the business of the system failing included review of:

- the updated Risk Register which includes third party suppliers' risks;
- the Recovery Plan;
- the final Clean Management Plan;
- the final Test Plan/Test Results;
- the latest Compliance Inventory;
- the Clean Management Audit Report;
- a Project Closure Document or plan for additional work.

Final Project Certification: the Final Compliance Certification Review Board considered the evidence on the readiness of the project, the quality of the supporting documentation, the quality of the clean management regime and the adequacy of the recovery plan. Failure to satisfy the Board on any of the review points led to a plan of action and requirement for another application for final certification.

Assessment Results

The National Audit Office carried out their second assessment in September 1999. The review team found that the final certification process had been completed and that there was sufficient evidence of readiness to support a rating of blue for all of The Met. Office services identified in the Action 2000 national infrastructure model.

Case Study: Independent Assessment at the Met. Office *continued*

Business Continuity

The Met. Office has reviewed its Business Continuity arrangements to ensure that the specific risks relating to operations over the millennium are adequately covered by a range of additional preventative and contingency measures designed to ensure that key services (in particular those critical to defence and national infrastructure) are protected from disruption.

The business continuity plan includes a **Millennium Operating Regime** that provides a large array of enhancements to normal operations, including:

- increased manning at critical sites;
- an Executive Management and Response Team;
- enhanced recovery plans for critical systems and sites;
- enhanced fall back redundancy in production networks;
- extra payments for staff.

The Met. Office tested the Executive Management and Response Team and operated it "live" over the night of the 8th/9th September. No "9999" problems were found. This team also participated in the Cabinet Office's exercise of infrastructure reporting arrangements held on 26 October.

What about businesses not assessed as part of the essential services of the UK?

2.11 Outside of the UK national infrastructure assessments, Action 2000 have undertaken regular research on the readiness of businesses through surveys with business leaders and Year 2000 managers. Survey results published in September 1999, based on 2022 interviews conducted in August by independent researchers, show an improving position in the numbers considered to be on track:

- 91 per cent of larger businesses (those with more than 250 employees);

- 73 per cent of businesses with 10 to 249 employees (up from 65 per cent in June 1999).

2.12 Action 2000 did not survey businesses with one to nine employees in this round, but the previous survey in June, with the results published in August, showed 54 per cent considered to be on track.

2.13 Although the survey results published in September are encouraging, still more than one-quarter of businesses with 10 to 249 employees had an identifiable risk, but are not taking the full range of steps to address Year 2000 issues.

2.14 The survey also revealed slow progress in developing and completing continuity plans. Figure 10 summarises the results. Overall, the concern is that some of these businesses may experience millennium bug failures.

Figure 10

Continuity planning in UK businesses: September 1999

Businesses with 10-249 employees

3%
13%
6%
41%
37%

Businesses with 250+ employees

35%
48%
4%
2%
11%

■ Completed ■ Intended
■ Underway ■ Recognise need to do so
■ Considered unnecessary

Source: Action 2000 "Wave 7" survey results
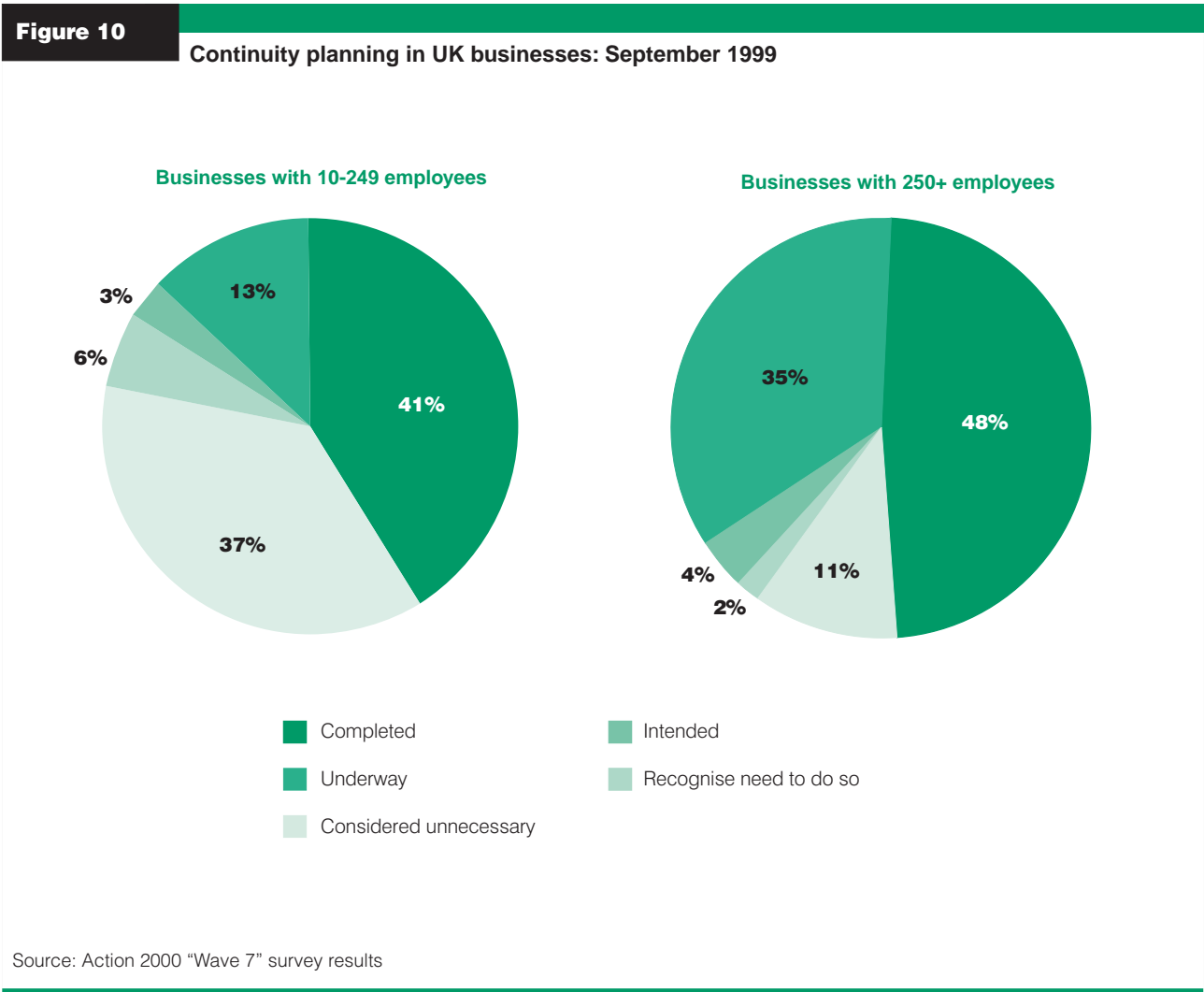
2.15 Further information is on the Action 2000 Internet web site (http://www.bug2000.co.uk). Figure 11 is a case study of a millennium operating regime in the private sector (Sainsbury's).

Case Study - How a private sector organisation has planned its millennium operating regime

### Figure 11

Sainsbury's

Introduction

1. J Sainsbury plc has been planning for the millennium date change since 1995 and has spent over £55 million on its Year 2000 programme, run by two dedicated teams (IT and non-IT), each headed by a senior manager seconded from the business. As part of this work 6,500 suppliers and 900 Sainsbury's retail outlets and sites were evaluated. This case study shows the steps the company has taken to ensure the smooth running of its business leading up to and beyond the millennium weekend.

Planning

2. Sainsbury's set up 11 working groups, one in each of the key business areas, to carry out risk assessment and impact of threats on the business in the areas of IT systems, Infrastructure and the Supply Chain. For example, there were working groups for retail, procurement, petrol filling stations, finance and communications.

3. The working groups carried out self-assessments based on guidance provided by a Business Continuity Team and target dates for readiness were set. They also produced documented contingency plans to address known Year 2000 threats. For example, in the event of problems with suppliers of more exotic products, there are contingency plans to buy substitute products from UK growers. The responsible Director from each of the business areas had to sign a statement that everything necessary had been done and that readiness had been achieved.

The Millennium Operating Regime

4. Work on the Millennium Operating Regime (MOR) started a year ago. The core time span for the MOR is 8.00am, 31 December 1999 to 12.00 noon, 3 January 2000. All stores will close at 4.00pm on 31 December and re-open on 3 January 2000. The diagram below summarises the main teams and areas of the business involved in the MOR. The Business Continuity Team is responsible for identifying and spreading best practice and training staff on MOR issues.

Sainsbury's Millennium operating regime
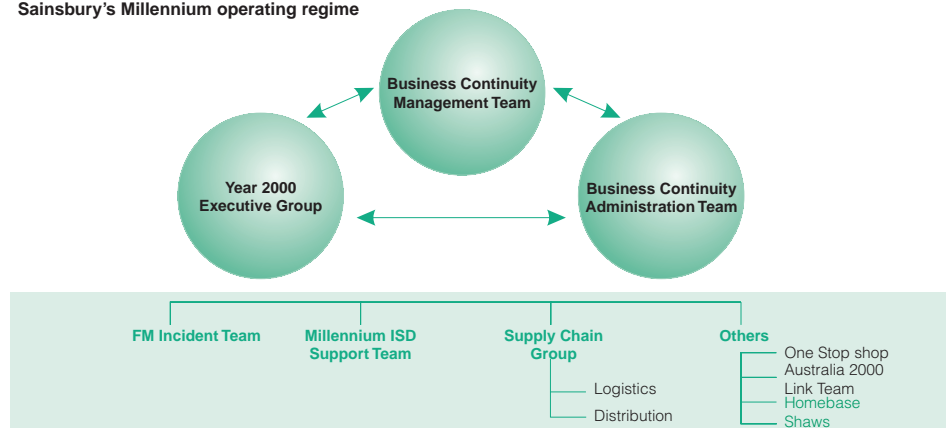
Business Continuity Management Team

Year 2000 Executive Group

Business Continuity Administration Team

FM Incident Team

Millennium ISD Support Team

Supply Chain Group
- Logistics
- Distribution

Others
- One Stop shop
- Australia 2000
- Link Team
- Homebase
- Shaws

Case Study - How a private sector organisation has planned its millennium operating regime
continued

Figure 11

5. Sainsbury's has produced a comprehensive and robust MOR, which has been thoroughly tested twice (August and October 1999) and improved as a result of each test. The tests consisted of a 7 hour simulation exercise attended by around 50 key staff who will be on duty over the core MOR period. Working in dedicated support teams around a central Business Continuity Administration Team, participants were faced with rapidly developing scenarios specific to their own specialist areas which could arise during this period. Scenarios included product recall due to a quality control problem, power failures at supermarkets and fire at key depots. Full evaluation and corrective action was taken after each exercise and results were fed to the management of all retail outlets and sites.

6. The main measures taken to ensure the smooth running of business over the millennium period include:

    ■ sending out a team of two to a similar company in Australia, a week in advance, to monitor any problems encountered and to provide advance warnings and reports to Sainsbury's in the UK. The assumption is that problems encountered in the UK are likely to be similar to those in Australia;

    ■ staffing the Head Office at Blackfriars by between 50-70 key personnel, including ten staff in a central control room with emergency equipment, such as, computers, help desks, mobile phones and radios. An IT helpdesk will also be located at Blackfriars. A second infrastructure helpdesk will be based at Uxbridge to resolve problems such as breakdown in refrigeration. Should either of these control rooms fail, a location in Hertfordshire could be used as a command centre;

    ■ staffing each retail outlet over the millennium period with two to three personnel;

    ■ issuing management teams of all retail outlets and sites with a package of instructions, including a long list of checks which are required to be carried out over the millennium period, such as equipment and systems checks, at specified times and procedures for reporting the results;

    ■ a remuneration package for all staff on duty over this period, consisting of lump sum payments and additional holidays'.

    ■ working with the high to medium impact suppliers to resolve potential supply chain problems.

    ■ holding additional stocks in all supermarkets of ten key "bunker" lines, such as bottled water, orange juice, UHT milk, tea, tomato soup and cornflakes. Sainsbury's has worked with suppliers to ensure that a second list of further additional stocks will be kept in supply chain and it is anticipated that a third list will be kept by the suppliers themselves. These lists have been discussed with the Institute of Grocery Distribution and the Ministry of Agriculture Fisheries and Food, and have been based on extensive in-house research and forecasting models;

    ■ easing the pressure on business over this period through various actions such as undertaking payroll a week early and freezing software and hardware systems (October and November, respectively);

    ■ keeping the public fully informed of their plans through customer leaflets and updates on their website.

7. Sainsbury's has agreed to report to the Ministry of Agriculture Fisheries and Food as part of the Government-wide millennium operating regime on the current state of play every four hours over the core millennium period. It has also agreed to pass on the reports received from its team in Australia.

How have citizens and businesses been kept informed?

2.16 Action 2000 and Government have undertaken a series of publicity campaigns to provide the public with information about the millennium bug and the readiness of the UK. Recent focus has been on publicising the results of the independent assessments of the readiness of the national infrastructure through a series of colour advertisements in the national press (in May, July and October 1999). In addition, a "Facts not Fiction" booklet distributed with national newspapers and magazines in June 1999 aimed to provide background information, point to sources of further information, and dispel some of the fiction that has grown up around the millennium bug. A further booklet is being delivered to every home in the UK in the week commencing 8 November.

2.17 The responsible body for each sector takes the lead on publicising readiness of the sector and the processes within it, and is responsible for encouraging individual companies and service providers to publicise regional and local readiness.

2.18 For businesses, Action 2000 have a continuing programme to raise awareness and promote Year 2000 remedial and continuity work including booklets for factories and schools. In September 1999 they launched a "Last Chance" guide to focus businesses on areas critical to their survival and provide guidance and checklists for businesses at all stages of preparedness.

Conclusions

Will essential services be disrupted as a result of the Year 2000 problem over the millennium period?

2.19 The work of Action 2000 to assess progress towards "no material disruption" in essential services for the UK national infrastructure continues to focus attention on key service providers over both public and private sectors. The scope of the programme of assessments has been extended to cover business continuity planning and millennium operating regimes.

2.20 Successive disclosures show continuing good progress with most sectors now rated 100 per cent blue (no identified risk of material disruption). For those sectors with an amber rating – some risk of material disruption, but agreed containment plan in place – responsible bodies report that work is in hand to ensure a 100 per cent blue rating is achieved in good time.

2.21 The focus given to the key processes of the UK national infrastructure means that the risks of major failures arising are low. However the level of response from businesses outside the national infrastructure programme has not been as good, particularly for small and medium sized enterprises. There is thus some concern that these businesses may experience millennium bug failures.

Part 3: Progress by Central Departments and Agencies

Who is responsible for taking action to overcome the millennium threat in central Government Departments and Agencies?

3.1 For central Government Departments and Agencies, Departments are responsible for their own compliance programme. Individual Departments also lead on areas of the wider public sector and the private sector for which they have sponsoring interests.

3.2 Where we audit a body, we have sought a specific acknowledgement of accounting officer responsibilities for Year 2000 issues as part of the letter of representation to support their financial statements to ensure that Year 2000 issues are receiving proper attention at the highest level within all audited bodies.

Who is responsible for monitoring progress?

3.3 The Cabinet Office have an overview role to provide guidance on requirements, monitor and publicise progress, identify potential weaknesses, and suggest recovery action. Progress in larger central Departments and their Agencies has been monitored since initial Year 2000 action plans were completed in October 1997, and coverage of monitoring returns has been gradually extended both in the number of bodies surveyed and in coverage of the monitoring returns. Progress has been monitored quarterly, with monthly reviews from July 1999.

3.4 The progress reviews have supported a frequent series of Government statements to the House of Commons since November 1997. In August and September 1999, all MPs were advised of progress by letter.

3.5 Progress is monitored through the issue of questionnaires to Departments and Agencies. Data were collected a little earlier than the date of the statement it supports; for example the bulk of the data supporting the statement in September, and used in the analysis below, contained an element of forecasting of the position at the end of September.

3.6 The results, together with the Departments' and Agencies' original plans and other additional information, have been placed in the House of Commons Libraries and published on the Internet at

(http//www.open.gov.uk/citu/y2000.htm). In addition, some bodies have publicised their progress directly, for example through annual reports or their Internet web site.

3.7 These arrangements cover Scotland and Wales, with the Scottish Executive (before July 1999, the Scottish Office) and their Agencies and the National Assembly for Wales (before July 1999, the Welsh Office) providing returns. The National Assembly for Wales also provide a narrative summary return for their wider public sector, including local authorities and the National Health Service in Wales. We are reporting separately on Scotland and Wales in parallel with this Report. With the agreement of the Northern Ireland Office, the arrangements also cover Government Departments and Agencies in Northern Ireland. The summarised results are also published on the Internet at the address in paragraph 3.6, although progress in Northern Ireland is outside the scope of our Report.

Coverage of returns

3.8 The number of returns from central Government and Agencies has grown steadily from an initial 63, rising to 81 in March 1999 and to 91 by September. A full list is at Appendix 3. The level of detail continues to vary significantly, with some Departments submitting detailed returns for quite small bodies and others providing a much less detailed return covering a number of bodies.

Progress in meeting target dates

3.9   It was the Government's initial intention that all Departments should have modified and tested all modified systems by January 1999 (or April 1999 for financial systems). From all Departments and Agencies initially expecting to meet these dates, overall progress has slipped steadily. There has been a corresponding steady rise in the number of bodies expecting to finish the overall work after September 1999 (Figure 12).

Change in the number of bodies expecting to complete after September 1999

Figure 12
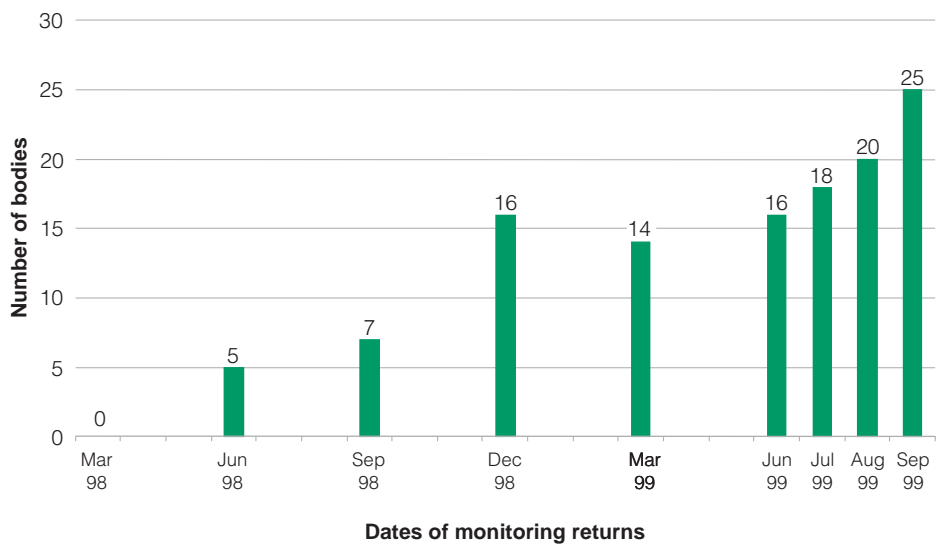
Source: Central Departments' and Agencies' monitoring returns

For example, for business critical IT systems, the percentage of bodies expecting to complete work by the target date had fallen from 100 per cent to 86 per cent by June 1998, and 37 per cent by March 1999. In the event only 30 per cent had finished that work by April 1999. At the time of completion of the September returns, only 52 bodies reported their work complete for all business critical systems. Of the others, since our last Report ("The Millennium Threat: 221 Days and Counting", (HC 436, Session 1998-99)), which drew on the March 1999 monitoring returns, six have brought forward completion and 26 reported slippage.

3.10 In the following paragraphs we highlight the conclusions drawn from our examination of the quarterly returns, in terms of:

- business critical systems (paragraph 3.11);

- non-critical systems (paragraph 3.12);

- availability of skills and resources (paragraph 3.14);

- compliance of the supply chain (paragraph 3.16);

- revising and testing business continuity plans (paragraph 3.18);

- creating and testing millennium operating plans (paragraph 3.20);

- overall cost estimates and spend (paragraph 3.22);

- independent validation of plans (paragraph 3.24).

Progress on business critical systems

3.11 For business critical systems, progress has been monitored under three categories, IT, embedded, and telecommunications systems:

- **business critical IT systems:** by September 1999, the number of bodies who are millennium compliant has increased to 54 (out of 86). Although the majority of bodies expect to complete work by the end of September 1999, there are six bodies expecting to complete final work from October to December 1999 (Figure 13);

- **business critical embedded systems:** by September 1999, the number of bodies who are millennium compliant has increased to 58 (out of 86). For four bodies work is expected to be completed in October 1999 or later (Figure 13);

- **business critical telecommunications systems:** by September 1999, the number of bodies who are millennium compliant has increased to 63 (out of 83). For three bodies work is expected to be completed in October 1999 or later (Figure 13).

Business critical systems: bodies with estimated completion dates from October to December 1999

Figure 13

Body

- Defence Procurement Agency
- Foreign and Commonwealth Office
- Ministry of Defence (Centre)
- Planning Inspectorate
- The Rent Service
- Royal Air Force
- Serious Fraud Office

Oct · Nov · Dec

■ IT Systems · ■ Embedded Systems · ■ Telecom Systems
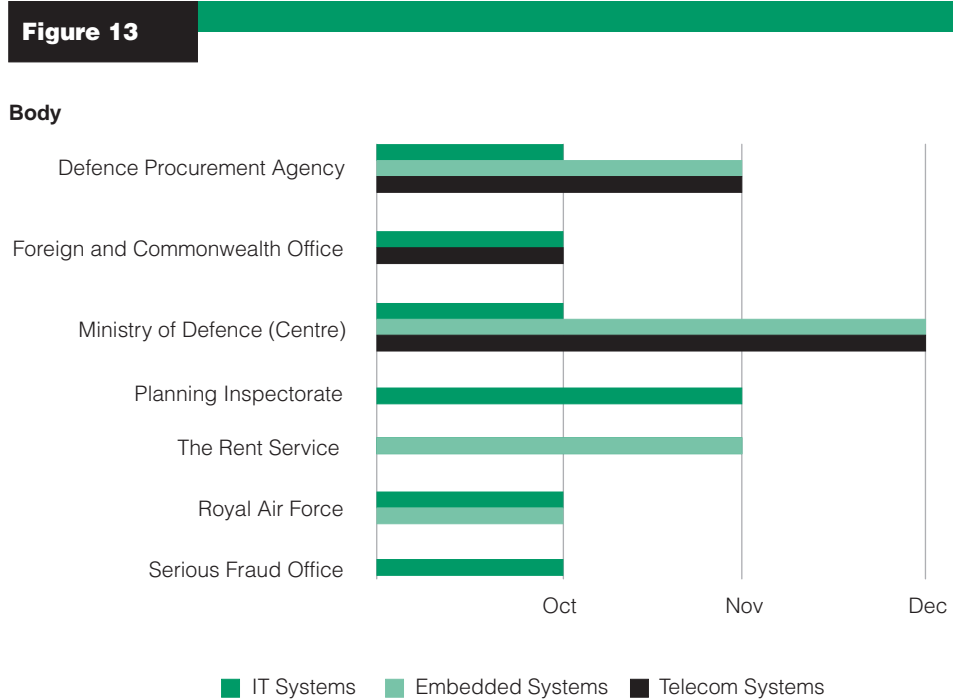
Source: Central Departments' and Agencies' monitoring returns

Progress on non-critical systems

3.12 By definition, non-critical systems have lower priority in a millennium programme. But their failure may still cause inconvenience and additional work. Successive monitoring returns also report significant slippage in this area.

3.13 Non-critical systems have again been categorised into IT, embedded systems and telecommunications systems:

- **non-critical IT systems:** the latest review shows that since March 1999 the number of bodies reporting compliance dates of October 1999 or later has risen from 10 to 20. These include the Vehicle Inspectorate and the Home Office (Centre) (both December 1999), nearly all of the Ministry of Defence (up to January 2000) and the Foreign and Commonwealth Office (March 2000);

- **non-critical embedded systems:** the latest review shows that since March 1999 the number of bodies reporting compliance dates of October 1999 or later has risen from seven to 14. These include the Vehicle Inspectorate and the Home Office (Centre) (both December 1999), most of the Ministry of Defence (up to December 1999) and the Foreign and Commonwealth Office (March 2000);

■ **non-critical telecommunications systems:** the latest review shows that since March 1999 the number of bodies reporting compliance dates of October 1999 or later has risen from four to seven. These include the Home Office (Centre) (December 1999) and parts of the Ministry of Defence (up to December 1999).

Availability of skills and resources

3.14   Over the past two years, many commentators have warned that the fixed deadline for achieving millennium compliance would increase competition for skills and resources and drive up salaries and prices, and forecast that in some cases staff resources necessary would not be available. This aspect has been monitored since February 1998.

3.15   Since June 1998, the number of bodies reporting insufficient resources to carry through compliance work has fallen steadily with only four bodies (Army, Forestry Commission, Hydrographic Office and Ministry of Defence (Centre)) reporting a shortage in the September 1999 returns. Others reported that shortages had been overcome by re-prioritising or delaying other work and obtaining outside assistance. By September 1999 about a third of bodies were delaying or cancelling other work.

Percentage of bodies reporting inadequate resources

Figure 14

Dates of monitoring returns
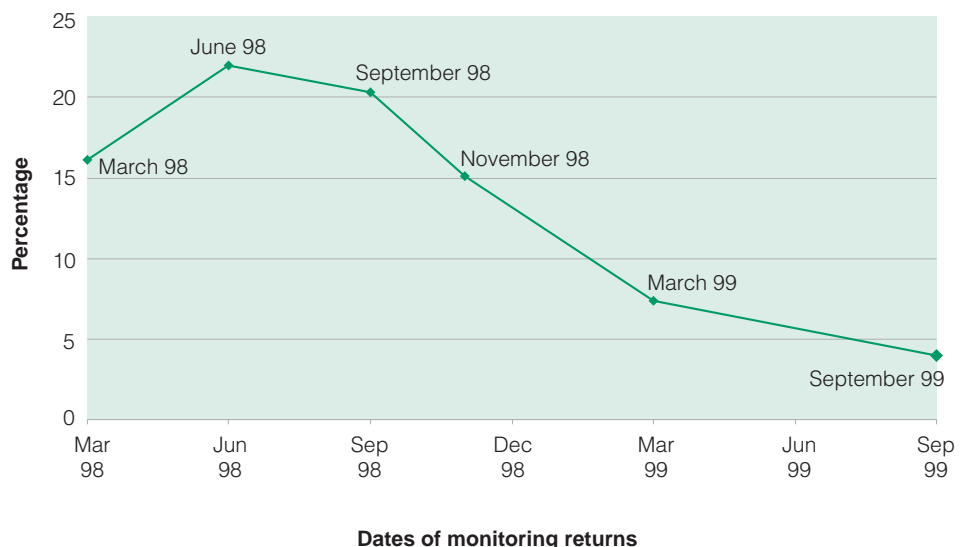
Source: Central Departments'
and Agencies' monitoring returns

Compliance of supply chain

3.16   Monitoring of this aspect of Year 2000 work has been expanded from general assurances to more specific reporting on supply chains. Departments and Agencies are now asked to report whether members of the supply chain have given:

- assurances that IT products and embedded systems supplied from outside are millennium compliant;

- assurances that general suppliers are themselves millennium ready, and that they will continue to function over the century date change together with concrete proof of such readiness.

3.17   The September 1999 returns showed a very mixed picture - assurances ranged between zero and 100 per cent for a body's IT and embedded systems products and from their general suppliers. Worryingly, fewer reported having received concrete proof of readiness.

Business continuity planning

3.18 In response to the Report from the Committee of Public Accounts (66th Report, 1997-98), the Cabinet Office asked all Departments and Agencies to develop initial business continuity plans by January 1999, and to update them during the year. The Cabinet Office subsequently asked for full, final and robust business continuity plans to be in place by October 1999.

3.19 By the September 1999 return, a little over half declared their plan as complete, but nearly all expected to complete it by the October 1999 target date. However, two-thirds of the plans, including many declared to be complete, had not been tested (Figure 15).

Figure 15

Progress in developing business continuity plans: position reported in September 1999 returns

Key aspects of business continuity plans

Percentage of bodies responding "yes"
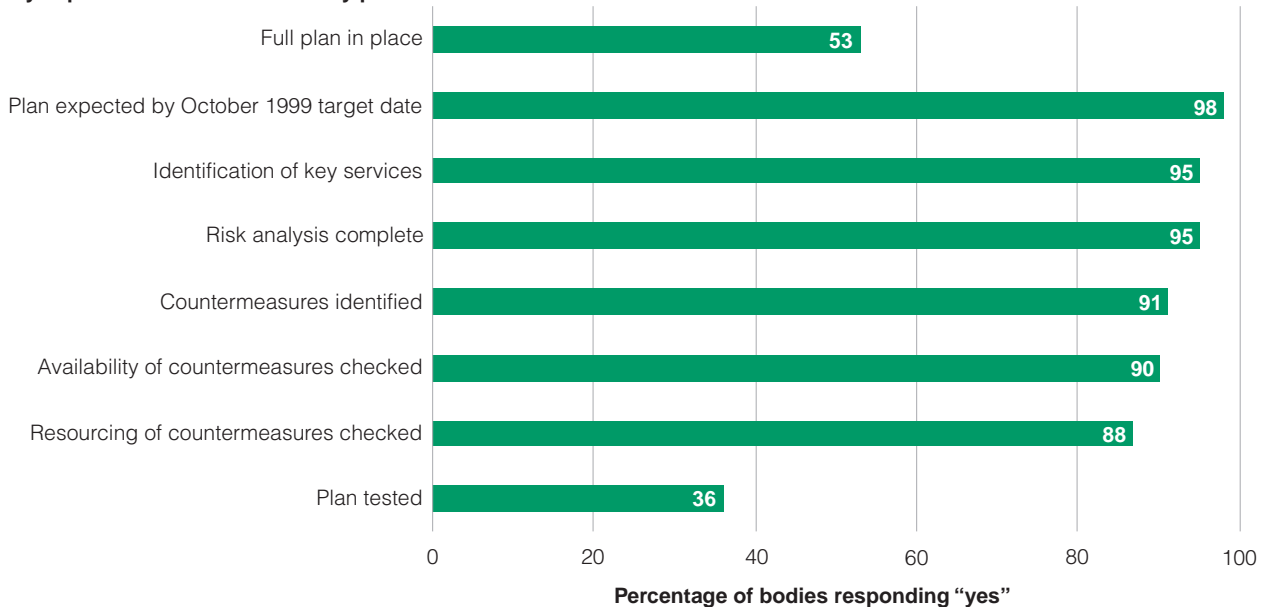
Source: Central Departments' and Agencies' monitoring returns

Millennium operating regime

3.20 The September 1999 return asked, for the first time, about the steps respondents had taken to achieve smooth running over the millennium period. Again, a little over 60 per cent declared their work in this area as complete, but although a number then lacked at least one of the suggested elements, nearly all expected to complete it by October 1999 (Figure 16).

Figure 16

Progress in developing millennium operating regimes: position reported in September 1999 returns

Key aspects of millennium operating regimes

Percentage of bodies responding "yes"
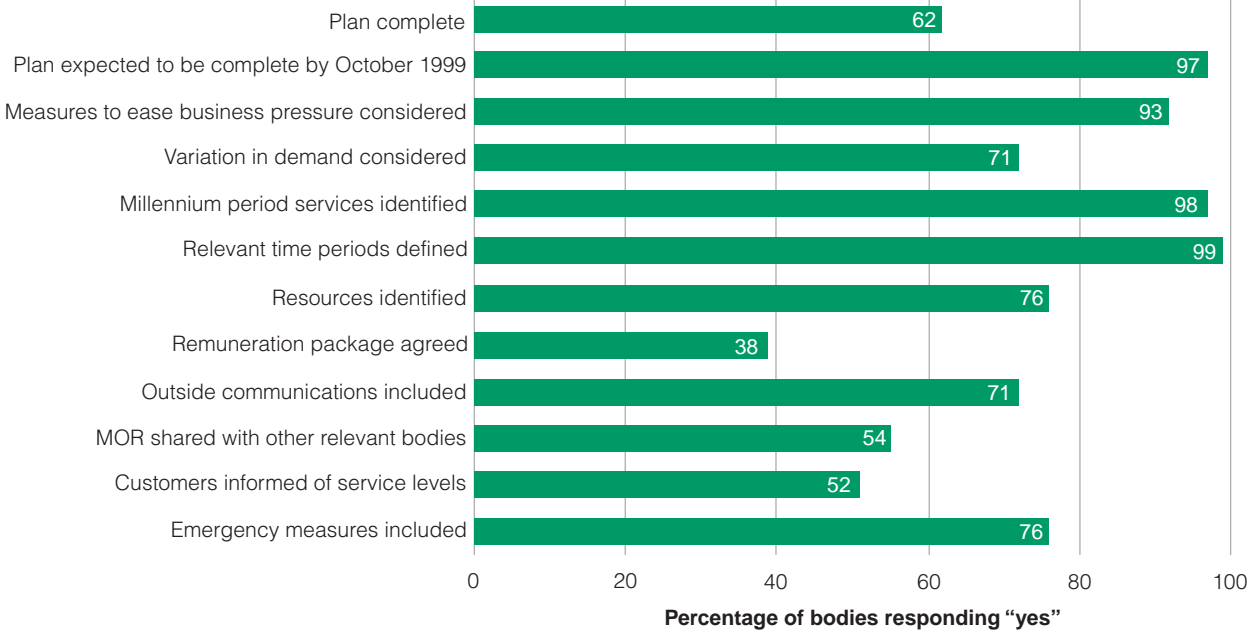
Source: Central Departments' and Agencies' monitoring returns

Overall readiness of bodies with late completion dates for business critical systems

3.21 For those bodies with completion dates for business critical systems from October to December 1999 (shown in Figure 13), focus on business continuity planning and planning their millennium operating regime is critical. Figure 17 shows the status of their business continuity plans and millennium operating regimes. Five of the seven bodies with late completion dates have also not completed this work.

Status of business continuity plans and millennium operating regimes for bodies with completion dates for business critical systems from October to December 1999

Figure 17

Body	Status of Business Continuity Plan (see Figure 15)	Status of Millennium Operating Regime (see Figure 16)
Foreign and Commonwealth Office	Completion predicted in October. Plan being tested.	Completion predicted in September. All posts overseas have prepared and tested individual plans.
Ministry of Defence (Centre)	Complete.	Complete.
Defence Procurement Agency	Completion predicted in September. Not tested.	Declared complete, but "customers informed" missing.
Royal Air Force	Complete.	Complete.
Planning Inspectorate	Completion predicted in August. "Identification of key services" not agreed. Plan not tested.	Declared complete, but "outside communications" missing.
The Rent service	Complete not tested	Completion predicted in October
Serious Fraud Office	Complete. Not tested.	Completion predicted in October. Six elements missing.

Overall cost estimates

3.22 In March 1998 Departments and Agencies making returns estimated the cost of millennium compliance work at £393 million. By March 1999 the overall final estimate had risen to £420 million, and by September 1999 to £434 million.

3.23 Although we recognise the difficulty in identifying and isolating the costs of Year 2000 compliance work from other activity, particularly when associated with work that would have been undertaken in any event, it is clear from returns that costs have not been reported on a consistent basis. For example, some Departments exclude in-house costs, others include the costs of the IT section but not those of users.

Independent validation

3.24 All bodies have had a review carried out independently of those undertaking the work. The latest returns show 82 per cent have been subject to an external assessment and the remainder to an internal one (for example by internal auditors). However, around 10 per cent of these reviews were completed before the beginning of 1999, when business continuity plans were not finalised and work on millennium operating regimes had not started.

Conclusions

Will central Government Departments and Agencies be ready on time?

3.25 Although considerable progress has been made since the position reported in our last Report ("The Millennium Threat: 221 Days and Counting", HC 436, Session 1998-99), slippage continues. At the time of our last Report eight bodies reported completion dates of October 1999 or later for business critical systems. The September returns show that there are still seven bodies in the danger zone where there is no room for further slippage.

3.26 Due to slippage, the number of bodies expecting to complete work on non-critical systems after September 1999 has increased from 10 to 20 since our last Report. This will inevitably cause inconvenience and additional work.

Do Departments and Agencies have the necessary skilled staff?

3.27 A shortage of resources is no longer a major issue, but it is work in other areas that has been deferred or slowed down to accommodate Year 2000 work and the impact of this will spill over into 2000.

Are continuity plans and millennium operating regimes in place?

3.28 Progress on continuity planning appears to be good, with nearly all bodies expecting to complete plans by the target date of October 1999. However, in September 65 per cent of plans had yet to be tested, and this may lead to additional work being identified.

3.29 Progress in devising millennium operating regimes, which flow from business continuity plans, has been very good, with 97 per cent of bodies expecting to complete plans by October 1999. But again, further work is needed to refine and enhance those plans.

3.30 Five of the bodies in the danger zone for completing work on business critical systems do not have fully completed and tested plans in place, adding further to the possibility of failure of some of their processes.

What will it cost?

3.31 Cost estimates reported have again increased from £420 million at the time of our Report "The Millennium Threat: 221 Days and Counting", (HC 436, Session 1998-99), to £434 million. There are some inconsistencies in reporting, and so this is likely to be an under estimate of the true cost of the work.

Is the public being kept informed?

3.32 Progress continues to be reported to Parliament regularly, and is published on the Internet, and attracts some media interest. Some bodies have publicised their Year 2000 progress directly.

Part 4: Emergency planning

Introduction

4.1 This part examines:

- who is responsible for emergency planning in the United Kingdom;

- existing emergency planning arrangements;

- how those arrangements have been enhanced to take account of the millennium;

- the readiness of the emergency services;

- the central Government's arrangements for monitoring the millennium bug and other problems over the millennium period.

Who is responsible for emergency planning in the United Kingdom?

4.2 The Home Office have primary responsibility for civil emergency planning in England and Wales. They co-ordinate emergency planning activity at both central and local Government levels in close co-operation with the emergency services. They also promote UK civil protection interests in NATO and the European Union.

4.3 At the local level, the concept of Integrated Emergency Management (IEM) applies. This brings together local authorities, the emergency services, healthcare providers and voluntary organisations who co-operate to respond to incidents which may cross over administrative and departmental boundaries. The Home Office pay a grant towards the emergency planning expenses incurred by county level local authorities in England and Wales, which supplements the commitment made by local authorities themselves. Similar arrangements apply in Scotland.

4.4 At the central Government level, there are two main elements in the arrangements for co-ordinating the response of central Government to emergencies: the Lead Government Department and the Civil Contingencies Committee.

4.5 The Lead Government Department is nominated to co-ordinate the response at central Government level, briefing Ministers, providing the framework within which individual Departments can discharge their statutory responsibilities and keeping Parliament and the public informed on progress in coping with the effects of the emergency. Lead Government Departments have already been nominated for a range of disasters or emergencies (e.g. MAFF, and their territorial counterparts in Scotland, Wales and Northern Ireland, for coastal or riverine flooding; Home Office for satellite incidents). Where there is no existing pre-nomination, or where there is uncertainty, responsibility for ensuring that a Lead Government Department is nominated in good time rests with the Cabinet Office. The decision normally depends on the nature of the disaster, and specifically any links to the normal business of a particular Government Department, and on ready access to information.

4.6 The Civil Contingencies Committee is a group of Ministers and officials that meets when necessary under the chairmanship of the Home Secretary, and provides a forum for the resolution of problems that cannot be resolved by the lead Government Department. The Committee's terms of reference include co-ordinating the preparation of plans for ensuring the supplies and services essential to the life of the community in an emergency; keeping these plans under regular review; and supervising their prompt and effective implementation in specific emergencies. It is on permanent standby should an emergency occur.

4.7 These responsibilities are illustrated at Figure 18.

Responsibilities for emergency planning

Figure 18

Civil Contingencies Committee
Chaired by Home Secretary
Emergencies that cannot be handled by the Lead Government Department

Home Office
Primary responsibility for civil emergency planning in England and Wales including co-ordination at both central and local Government levels

Lead Government Department
Co-ordinate response at central Government level

Local Level
Local Authorities
Emergency Services
Healthcare Providers
Voluntary Organisations

Source: National Audit Office

An overview of emergency planning arrangements

4.8 There are comprehensive and well developed arrangements in place for dealing with emergencies in the United Kingdom, based on flexible local arrangements to deal with any major hazard, whatever the cause. The main objective is a local response, which ensures that the appropriate resources and expertise are quickly brought to bear on any emergency.

4.9 Integrated Emergency Management (IEM) is a tried and tested concept, which brings together all of those who have a contribution to make. Local authorities, healthcare providers, the emergency services and voluntary organisations co-ordinate and co-operate together to respond to incidents which may well cross over administrative and departmental boundaries.

4.10 The underlying principle in the development of a plan is the response to any incident or emergency, and not its causes. This is recognised in emergency planning, which promotes flexible and integrated arrangements that can be incremental within an organisation's everyday working structure. The main planning stages associated with any emergency plan are illustrated at Figure 19.

**Main planning stages
of an emergency plan**

Figure 19

- Assessment
- Prevention
- Preparation
- Response
- Recovery
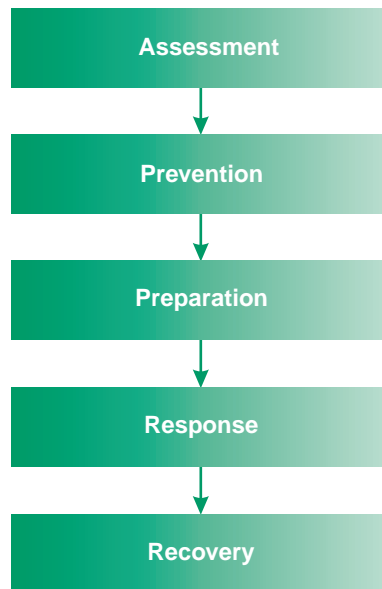
Source: Home Office

4.11 The different Agencies and organisations concerned with responding to emergencies have a greater or smaller contribution to make during each of these stages. For example, the Police co-ordinate the activities of all of those responding at the scene of the emergency, but the primary responsibility for the health and safety of those within the inner cordon at the emergency scene falls to the Fire Service. The role of the local authorities becomes more prominent as the emphasis switches to recovery. The local authority also leads on issues such as facilitating the rehabilitation of the community and restoration of the environment.

4.12 Management of the response to an emergency or disaster is undertaken at one or more of the following three levels:

- **operational level** (known as Bronze) - small, localised emergencies may be handled at the operational level only, generally at the scene of the emergency itself, without the need to invoke procedures at the tactical and strategic levels;

- **tactical level** (known as Silver) - invoked for more serious incidents when, for example, decisions have to be made about priorities in allocating resources. Tactical command is normally undertaken from an Incident Control Point, established in the vicinity of the incident site;

- **strategic level** (known as Gold) - only needed infrequently for major emergencies. Establishes a strategic framework within which tactical decisions can be made. The Strategic Co-ordinating Group is normally located away from the incident site, for example at Police Headquarters.

4.13 An illustration of a typical organisational approach for dealing with an emergency is at Figure 20.

4.14 Although the first response to an emergency is at the local level, there are occasions when the scale of an emergency goes beyond the capacity of local resources to cope. In these circumstances, recourse is made in the first instance to the services in adjacent areas through locally agreed mutual aid arrangements. However, there are also occasions when central Government has a role to play. Obvious examples might include providing specialist assistance not available locally or dealing with parliamentary, media or public enquiries.

Enhanced arrangements and activities for handling the millennium date change

4.15 The millennium bug and millennium celebratory events add to the potential for problems or emergencies over the New Year period. Local mutual assistance arrangements may be limited by problems arising elsewhere. The approach has been to enhance the arrangements already in place by adding millennium-specific preparations and by increasing the normal level of activity, for example, by running additional courses at the Emergency Planning College for local authority staff, staff from utility companies and others.

Figure 20	Example of a typical organisational approach for dealing with a disaster or emergency

Operational - Inner Cordon
Police
Fire
Ambulance
Specialist Advisers

Incident Control Point
Police
Fire
Ambulance
Liaison

Tactical - Outer Cordon
Issues to be addressed at the tactical level
- casualty clearing
- ambulance loading point
- vehicle marshalling area
- body holding area

Strategic
Issues to be addressed at the strategic level
- media centre liaison point
- local authority reception centre
- survivor reception centres
- casualty bureau
- relatives' reception centre
- public enquiries
- receiving hospitals
- temporary mortuaries

Strategic Co-ordinating Group
Police
Fire
Ambulance
Other Agencies,
Local Authority, Military
Government Advisers

Lead Government Department

Source: Home Office

A special "Millennium Issue" of the Home Office *Exercise Planners, Guide* was published at the end of last year, and two special editions of the contingency planning magazine *Civil Protection* were also published.

4.16 The Civil Contingencies Committee have taken on central Government responsibility for co-ordinating preparations over the millennium period. As well as a programme of meetings scheduled in the run up to the end of the year, the Committee will be on enhanced standby on Millennium Eve and New Year's Day.

4.17 In addition, detailed work is taking place at many other levels. For example, the Home Office has reported to the Civil Contingencies Committee on the emergency planning facilities used by central Government Departments, to provide assurance on continuing effectiveness over the millennium period.

4.18 The Home Office have also undertaken a programme of visits covering 75 of the 144 local authorities in receipt of Civil Defence Grants. The programme was designed to assess their level of millennium contingency planning, and to identify and share good practice. This revealed that although approaches varied widely, good progress was being made with relevant issues addressed. In addition, a good practice guide was recently circulated to all local authorities, following completion of the programme. Its purpose was to highlight a range of important issues in completing local authority preparedness. These included resources issues, business continuity plans, senior staff and elected member involvement, call out arrangements, communications, and advice to the public.

4.19 The Emergency Communications Network (ECN) provides essential communication in the event of an emergency, and is one of the key components in central Government's contingency arrangements for the year-end. The ECN is a resilient switched voice network linking emergency planners and response co-ordinators of central Government, local authorities, and the emergency services. In additional to normal funding, an additional £1.5 million has been committed to the network over the past 12 months, to ensure millennium compliance, provide increased resilience and traffic capacity for the millennium and to increase the number of sites provided with the system.

4.20 A specific one-day exercise for Ministers, in the form of a meeting of the Civil Contingencies Committee, was held in May.

4.21 A case study of how Birmingham City Council are planning for the millennium period is at Figure 21.

Case Study - Planning for the millennium period and celebratory events in Birmingham

Figure 21

Birmingham City Council Economic Development

Introduction

1. This case study looks at how Birmingham City Council have planned for the millennium period and events. It sets out the scale of the task, the planning and co-ordination arrangements and testing of the plans.

Scale of the task

2. Birmingham City Council's Year 2000 Project Team, headed by the Director of Environmental Services, has spent almost three years resolving millennium bug problems. All business critical systems have been made compliant and tested in a Year 2000 environment. Rectification work to resolve outstanding embedded chip issues will be completed by October 1999.

Figure 21

Millennium Emergency Planning Arrangements

10. Millennium Emergency Planning work started at the beginning of 1999 when Birmingham City Council's Emergency Planning Officer joined the Year 2000 Steering Group.

11. Birmingham City Council's existing business continuity and emergency plans cover scenarios such as loss of resources or facilities as a result of a natural disaster (fire or flood), system failure (loss of computer centre) and human error. Emergency planning for the millennium is much broader in scope given the potential scenarios, such as:

   ■ call centre and supporting systems are overloaded by the massive increase in call;

   ■ multiple failures occurring simultaneously;

   ■ loss of major service provider e.g. one or more of the utilities;

   ■ the cumulative effect of many small failures;

   ■ all services stretched to the limit;

   ■ inherited problems from other organisations. No support from elsewhere (i.e. any mutual aid);

   ■ large number of 'Events' taking place at the same time diverting resources;

   ■ streets will be closed causing access problems;

   ■ greater risk of disaster occurring.

12. The Millennium Emergency Plans have been tested twice. The first test took place in May 1999 and raised a number of issues, such as the impact of running an emergency without telecommunications being available. The test was extremely useful in refining planning assumptions.

13. The second more comprehensive test was carried out in September 1999. This involved all members of the Stewardship of Birmingham Group and lasted about five hours. The principal objectives of the exercise were to test:

   ■ the millennium contingency arrangements of Birmingham City Council and its departments;

   ■ liaison between all of the agencies involved;

   ■ evacuation;

   ■ transportation of evacuees out of the City centre;

   ■ handling the media;

   ■ short and medium term accommodation requirements.

14. Loss of telecommunications (including cell phones) was one of the scenarios in the exercise and participants quickly had to resort to alternative means of communication, including radios. The test showed that continuity was possible but that the radio network system required upgrading and further training in the use of radios was necessary. A final test of radio communications may be carried out before the end of the year.

Case Study - Planning for the millennium period and celebratory events in Birmingham *continued*

Figure 21

3.   Birmingham City Council are also planning a major programme of celebratory events in the City Centre over the millennium weekend. The celebrations will commence at 8.00pm on New Year's Eve, with the lighting of the Millennium Flame by Sir Cliff Richard, followed by an extensive music programme and spectacular laser show at midnight. The music programme will continue throughout the weekend. A crowd of over 50,000 is expected on New Years Eve in the City Centre. In addition, hundreds of smaller events will be held locally outside of the City Centre. The celebrations will place additional demands on emergency services.

Wider planning and co-ordination for the millennium period

4.   Planning for the wider issues surrounding the Millennium began in October 1998 when 'The Stewardship of Birmingham Group' was formed to undertake contingency planning. The group comprises 16 public and private sector organisations which have a major impact on the citizens of Birmingham and include the emergency services, NHS, utilities, transport providers, representatives from the Government Office for the West Midlands and military. They have met regularly and have been aware of each others progress towards readiness throughout, with each organisation preparing and sharing their position statements. All members of the Stewardship Group achieved blue status under the Action 2000 traffic light rating system by October 1999.

5.   In addition, a Year 2000 Group was set up, consisting of Year 2000 Officer Groups from individual local authorities within the West Midlands and surrounding counties. The Group has grown from nine to 17 authorities. Members exchange information and best practice on various aspects such as risk assessment methodologies and testing strategies.

6.   Before beginning contingency planning Birmingham City Council undertook a comprehensive Risk Analysis exercise. Detailed corporate guidelines for formulating millennium plans were issued to all service departments who produced their own individual plans, including resourcing requirements and call out lists. The main objectives of this exercise were to ensure that no clients or staff would be put at risk, and that both essential services and business as usual can be maintained. Based on this work Birmingham City Council agreed their millennium service priorities by April 1998.

7.   Given the special nature of the Year 2000 problem a basic planning assumption was made that little or no mutual aid would be available from neighbouring groups or authorities and Birmingham City Council sought to enhance the number of their own staff on call.

Planning for the millennium celebrations

8.   Planning for the Millennium celebrations commenced in January 1999 using a dedicated and experienced Events Team from Birmingham City Council's Leisure Services Department. The team has liaised closely with all parties involved, such as the emergency services, event organisers, voluntary groups (e.g. Community Action Network and Birmingham Voluntary Services Council), other Council departments and the Year 2000 project team.

9.   Specific measures to ensure the smooth and safe running of the celebrations include agreeing special arrangements with local transport operators. Birmingham City Council has also liaised with the local police on strategic road networks for clear access in case of emergencies.

Figure 21

Co-ordination of activity on New Year's Eve

15. On New Year's Eve, the Police will be opening a strategic level (Gold) co-ordinating centre to monitor events over the Millennium period. A representative of Birmingham City Council will attend once an emergency has been declared. A tactical control (Silver) centre will also be opened for the 'Events'.

16. The Director of Environmental Services will lead a small central co-ordination team on duty over the millennium weekend. This team will be based at different location to the Gold Control centre and will provide the interface with the emergency and other services and will form the Council's core emergency planning and co-ordination group and prioritise any contingency planning response which is required. Other key Chief Officers on call will be the Directors of Transportation, Housing and Legal Services. The Chief Executive will be available in the City during the weekend and will be contactable by mobile phone and by other arrangements. A small team from the Government Office for West Midlands will also be on 24-hour duty over the Millennium weekend.

Readiness of emergency services

Fire

4.22 The emergency services have incorporated special arrangements into their planning for the year-end to meet its particular challenges. All Fire Brigades have undertaken a rigorous process of risk assessment as part of their millennium readiness planning on the basis that, as far as possible, it will be "business as usual" over the period.

4.23 The readiness of Fire Brigades has been independently assessed as part of the UK national infrastructure programme described in Part 2 of this Report. All Brigades were assessed as blue (no identified risk of material disruption) under the

Action 2000 traffic light system in October 1999. In England and Wales the "responsible body" is the Home Office (the Scottish Executive in Scotland), who commissioned Her Majesty's Fire Service Inspectorate as independent assessors. Results of assessments have been reported to Home Office Ministers in addition to the National Infrastructure Forum.

4.24   Brigades have made plans based on information about the number and type of millennium events being planned and the extra demands that might be imposed on them over the period. They have also liaised with other emergency services (Police, Ambulance etc.) and utility companies and have made and tested contingency plans to cover foreseeable failures. This planning should ensure that sufficient fire fighters are available throughout the millennium period to cover the additional workload.

Police

4.25   In the same way, the readiness of the Police service to cope with the millennium has been independently assessed by Her Majesty's Inspectorate of Constabulary with all forces rated as blue at the end of October. Individual forces have carried out extensive work to ensure their information and communications systems will be working, and that plans are in place to maintain a proper level of service to the public.

4.26   Critical business processes have been identified and prioritised and the impact of disruption to them analysed. Continuity plans at a local level exist to cover specific eventualities and set out detailed procedures to be followed. Planning for known events is already in place, drawing on existing expertise in policing public occasions. Contingency plans to deal with emergencies are ready, and the service has worked closely with its partners in central and local Government, the other emergency services and key services providers in public, private and voluntary sectors to ensure they are aware of each other's plans.

4.27   A Police National Information Centre will be open on a 24-hour basis from midday 30 December 1999 to 4 January 2000, or later if necessary. Based at New Scotland Yard, it will receive information directly from local forces on the situation in their areas, which can then be passed to the Home Office Emergency Operations Centre, and onwards to the Cabinet Office (paragraph 4.30), Ministers, other Government Departments, other emergency services and the media to provide an overall national picture.

Healthcare services

4.28   The readiness of Healthcare services has been assessed by the National Health Service Executive, working through its Regional Offices, with a team of independent consultants, in collaboration with the Audit Commission. Regional Offices assessed each National Health Service (NHS) organisation through regular monitoring returns, supplemented by other information, and a NHS Executive central Year 2000 team have provided assurance through a programme of visits to NHS organisations. The Audit Commission provided further assurance through its programme of visits. The assessment process included helping ensure that those organisations that were behind with their Year 2000 programmes could catch up.

4.29   In October 1999, all organisations were rated blue. The NHS Executive has also issued guidance on measures to ensure that this compliance status is not compromised by any subsequent changes. The NHS Executive also created a Millennium Executive Team to co-ordinate planning for the coming Winter through a "Winter 2000" programme to ensure that the NHS copes with the usual pressures arising in Winter as well as the effects of the millennium. This includes a national communications campaign to provide public confidence in the NHS, encourage the best use of health services, and promote self-care where appropriate.

What are the Government arrangements for monitoring events over the millennium period?

4.30   Separately from the emergency planning arrangements, the Government will be monitoring events over the millennium period both nationally and internationally through a Government wide millennium operating regime. A Centre co-ordinated by the Cabinet Office will undertake monitoring. The main objectives are to collect and analyse information about:

- millennium bug problems in all sectors of the UK national infrastructure;

- international Year 2000 problems;

- other problems and difficulties arising over the millennium period which may or may not be millennium bug related;

in order to:

- brief Ministers;

- provide briefings for any meetings of the Civil Contingencies Committee;

- provide accurate and up to date information for the media;

- sign post the media to other information sources;

- provide information about the national picture to Government Departments and sectors contributing to the information network.

4.31 The Cabinet Office Year 2000 Team, the Media Co-ordination Unit and the Secretariat of the Civil Contingencies Committee will staff the Centre. But this will be a centrally co-ordinated information service, and will not disturb existing operational arrangements, particularly those for handling emergencies described earlier. These arrangements were tested on 26 October 1999 to ensure that they are both appropriate and effective.

4.32 In addition, each Government Department are required to have their own millennium operating regime covering:

- key services and processes;

- systems supporting them;

- operational needs over the millennium period;

- liaison arrangements with the sectors for which they have policy responsibility;

- provision of information to Ministers and the central Cabinet Office Unit;

- plans for providing public information over the period, including the ability to respond quickly and effectively to issues that arise unexpectedly.

4.33 The Cabinet Office Centre will receive information from Government Departments about sectors of the infrastructure for which they have policy responsibility. The Centre will also obtain assessments about the overseas position from the Foreign and Commonwealth Office which will receive information from both overseas posts and sectors with overseas links. The Centre will feed-back information on the national and international position to Departments and will also provide information to the media and public on the Cabinet Office web site (http://www.open.gov.uk/citu/y2000.htm). The Centre will be staffed from 31 December 1999 until 7 January 2000, with 24-hour operating arrangements, access to good communications including the Emergency Communications Network, and back up electricity generator facilities.

4.34 The relationship between these organisations and information flows is illustrated at Figure 22.

Figure 22   **Government millennium operating regime and information flows**
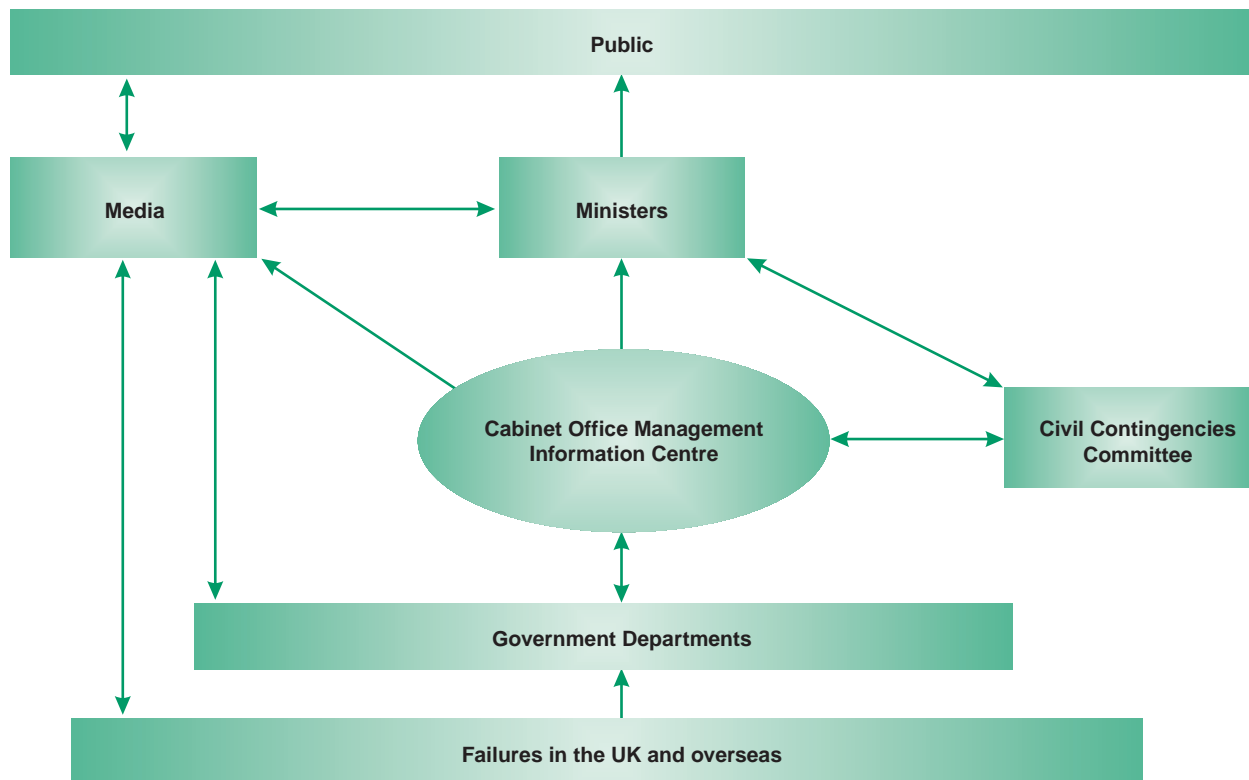
Source: Cabinet Office

Conclusions

Are emergency planning arrangements robust and adequately tested?

4.35 There are comprehensive and well-developed plans for dealing with emergencies in the United Kingdom, with clear roles established for local authorities, healthcare providers, the emergency services, key utilities and Government Departments. The concept of Integrated Emergency Management is tried and tested through routine exercises and dealing with genuine emergencies.

Have plans been adequately enhanced to deal with the millennium?

4.36 The Home Office have undertaken a great deal of work to enhance the normal arrangements to cater for the millennium both at local, Departmental and central Government levels, including conducting exercises to test plans up to and including Ministerial level. This recent experience will be invaluable if any emergencies do arise over the millennium period.

Are central Government monitoring arrangements comprehensive and adequately tested?

4.37 The Cabinet Office will be setting up a Management Information Centre as part of a Government wide millennium operating regime. This will collect and analyse information from Government Departments about the sectors of the infrastructure for which they have policy responsibility, and from the Foreign and Commonwealth Office about the overseas position. The Centre will provide an information feedback service to Departments, the media and the public. These arrangements were tested on 26 October.

Part 5: The overseas position

Who is responsible for assessing the overseas position?

5.1　In the modern global economy, key infrastructure sectors such as telecommunications, finance and transport have many points of interdependence, not least internationally. Year 2000 failures in one country could have knock-on effects in others.

5.2　The international elements of services delivered and consumed within the UK are included in the colour coding because they are assessed as part of the normal supply chain risk, and these risks are also assessed through business continuity plans. However, the foreign elements of services delivered or consumed outside the UK are not covered by the UK national infrastructure assessments reported in Part 2, and are not colour coded. This is because of the difficulty in gathering accurate and reliable information abroad, and because the rigour of the independent assessment of the process in the UK cannot be applied.

5.3　More widely, the Foreign and Commonwealth Office (FCO) are responsible for providing travel advice for the public travelling abroad, and advice to British businesses. In addition the FCO, with the Department of Trade and Industry and other Departments as well as Action 2000, have been co-ordinating action to assess and address risks to British interests from Year 2000 failures overseas. The FCO have also taken the UK lead on international action within the G8 and European Union fora.

What information is available on the effect on the UK national infrastructure?

5.4　Through their posts overseas, the FCO have sought to obtain as much information as possible on the position abroad for a small number of critical infrastructure sectors. For example:

- telecommunications, for which robust international links are a key element of many continuity plans;

- financial services, where most bodies have international links;

> the supply and distribution of food and essential goods, which is dependent, for example, on the operation of the port of Rotterdam, the motorway system in Northern Europe and the Channel Tunnel.

5.5 The aim of this work is, as far as possible, to appraise the key aspects of the international supply chain and publish the results, although not formally part of independent assessments.

5.6 At the National Infrastructure Form meeting on 21 October it was reported that preparations in these critical areas were well advanced. For example, the International Telecommunications Union reported that 40 countries, covering roughly 95 per cent of world wide telecommunications traffic, had participated in international telecommunications testing and that no Year 2000 faults had been uncovered. Similarly, for international financial services, Global 2000, with membership of 888 firms in 107 countries, reported on a series of successful testing of cross border payments and exchanges.

Advice for travellers and businesses

5.7 The FCO issued some general advice in March 1999 which warned of potential disruption caused by the millennium threat and advised travellers to seek advice from travel agents and airlines on how potential problems were being addressed at their planned destination.

5.8 In their Report "The Millennium Threat" (HC 517, Session 1998-99), the Committee of Public Accounts urged the FCO to make country specific assessments available as soon as possible. On 14 September, the FCO issued "country statements" and Year 2000 related travel advice notices for the top 50 countries most popular for trade and tourism, which account for more that 90 per cent of UK trade. Additional country statements are being published continuously. By the end of October the FCO had issued 114 country statements.

5.9 The country statements have been compiled from a range of public and other sources available to FCO staff both at overseas posts and in the UK. However, it is difficult to verify the accuracy, reliability and completeness of the information available from official and other sources, although FCO staff have attempted to do so where possible. In addition, any information provided may quickly become out of date. As a result, the FCO do not guarantee that the statements are accurate, definitive or exhaustive although regular updating is taking place when material changes occur to ensure that they provide the best quality information possible.

5.10 Overall the statements present a very mixed picture of progress. Some countries have identified risks to their infrastructure and have implemented assessment and rectification programmes. For others, systems failures affecting the infrastructure of the country are expected as a matter of routine and the attitude is very much to wait and see what happens over the millennium rather than take preventative action.

5.11 In addition, readiness of any particular country depends on a range of factors, for example, its dependence on IT systems in service delivery compared with manual systems, its culture in dealing with systems failures and "workarounds", as well as the willingness of both public and private sectors to undertake Year 2000 compliance work against other priorities.

5.12 The FCO statements and travel notices are available on the Internet at http://www.fco.gov.uk , and are provided to the public and businesses on request. An example of a country statement is at Appendix 6. A full list of the 131 countries for which statements are available is at Appendix 7. Despite the caveats, in the first two days alone, these information pages on the FCO web site attracted over 28,000 visitors, with 250,000 visitors recorded by mid October. This has demonstrated the demand for this information.

5.13 Other countries, including Australia, Canada and the United States, have also published their own statements on other countries, including on the Internet:

■ Australia – http://www.dfait.gov.au;

■ Canada – http://www.dfait-maeci.gc.ca;

■ United States – http://www.y2k.gov.

5.14 In addition, the Action 2000 web site (http://www.bug2000.co.uk) contains links to some 90 web sites around the world providing Year 2000 information from individual countries. The list is reproduced at Appendix 8, together with some other web sites providing Year 2000 information. Together these statements provide a wider range of information for the public to draw on. But this is material published by the sources specified, there is no guarantee as to accuracy or completeness, and users have to trawl through many sources to get a full picture.

Conclusions

5.15 The country statements issued by the FCO are a valuable addition to the information available elsewhere. However, the information is not, and can never be, of the same quality as that provided on UK national infrastructure processes. It is difficult for the FCO to verify the completeness or accuracy of the statements, they may give an incomplete picture of the position. In addition, any information provided may quickly become out of date although the FCO are taking steps to ensure that does not happen.

5.16 Businesses and travellers seeking advice on the millennium readiness of individual countries therefore need to trawl through a wide range of sources including local sources in the country concerned whenever possible to gain a full picture. Even then, no guarantee can be given of completeness or reliability.

Appendix 1: Year 2000 – a chronology

January 1997	Target date for central Departments and Agencies to complete audit of systems
21 May 1997	NAO Report "Managing the Millennium Threat published
September 1997	Action 2000 created
31 October 1997	Central Departments and Agencies completed initial cction plans
March 1998	Ernst and Young commissioned to identify national infrastructure processes and map key dependencies in the UK.
March 1998	1st Central Government monitoring return
March 1998	Government statement to the House of Commons
30 March 1998	Prime Minister's announcement of Government's objective to "ensure no material disruption to the essential services of the United Kingdom on which the public rely."
30 March 1998	Year 2000 team created in the Cabinet Office
15 May 1998	NAO Report "Managing the Millennium Threat II" published
15 June 1998	Committee of Public Accounts took evidence on NAO Report "Managing the Millennium Threat II"
June 1998	Audit Commission Report " A Stitch in Time" published.
June 1998	Central Government Quarterly Monitoring Return
June 1998	Government statement to the House of Commons
27 July 1998	Committee of Public Accounts Report "Managing the Millennium Threat" published
September 1998	Report on key processes and dependencies in the national infrastructure published.
September 1998	Central Government Quarterly Monitoring Return
September 1998	Government statement to the House of Commons
October 1998	National Infrastructure independent assessment programme started
13 October 1998	National Infrastructure Forum Meeting
November 1998	Audit Commission Report "Time Marches On " published
November 1998	Central Government Quarterly Monitoring Return
November 1998	Government statement to the House of Commons
21 January 1999	National Infrastructure Forum Meeting
January 1999	Target date for central Government Departments and Agencies to complete remedial work on non financial systems
January 1999	Target date for central Departments and Agencies to have initial business continuity plans in place
17 February 1999	NAO Report "How the Utility Regulators are addressing the Year 2000 Problem in the Utilities" published
March 1999	Central Government Quarterly Monitoring Return
16 March 1999	Government statement to the House of Commons
21 April 1999	National Infrastructure Forum Meeting
April 1999	Target date for central Government Departments and Agencies to complete remedial work on financial systems
12 May 1999	Committee of Public Accounts took evidence on NAO Report "How the Utility Regulators are addressing the Year 2000 Problem in the Utilities"
26 May 1999	NAO Report "The Millennium Threat: 221 Days and Counting" published
9 June 1999	Committee of Public Accounts took evidence on the NAO Report "The Millennium Threat: 221 Days and Counting"
June 1999	Central Government Quarterly Monitoring Return
18 June 1999	Government statement to the House of Commons
12 July 1999	National Infrastructure Forum Meeting
28 July 1999	Committee of Public Accounts Report "How the Utility Regulators are addressing the Year 2000 Problem in the Utilities" published

July 1999	Central Government monthly progress check
18 August 1999	Committee of Public Accounts Report "The Millennium Threat" published
August 1999	Central Government monthly progress check
September 1999	Central Government Quarterly Monitoring Return
23 September 1999	MPs advised of central Government progress by letter
21 October 1999	National Infrastructure Forum Meeting
October 1999	Central Government monthly progress check
October 1999	Target date for central Departments and Agencies to have completed and tested business continuity plans in place

Appendix 2: Reports by the Comptroller and Auditor General and the Committee of Public Accounts

Comptroller and Auditor General

Managing the Millennium Threat..HC 3, 1997-98

Financial Auditing and Reporting: 1996-97 General
Report of the Comptroller and Auditor General.......HC 251-XIX, 1997-98

National Health Service (Scotland)
Summarised Accounts1996-97......... ....HC 692, 1997-98

Managing the Millennium Threat II....................................HC 724, 1997-98

Appropriation Accounts 1997-98 Volume 16:

Departments of the Chancellor of the Exchequer..............HC 1-XIV, 1997-98

How the Utility Regulators are Addressing the
Year 2000 Problem in the Utilities.................................HC 222, 1998-99

National Health Service (Wales) Summarised Accounts
1997-98...HC 261, 1998-99

Financial Auditing and Reporting: 1997-98 General
Report of the Comptroller and Auditor General ....HC 1-XIX, 1998-99

National Health Service (England)
Summarised Accounts 1997-98 ....HC 382, 1998-99

The Millennium Threat: 221 Days and Counting ....HC 436, 1998-99

Committee of Public Accounts

Managing the Millennium Threat (66th report 1997-98).......HC 816, 1997-98

National Health Service (Scotland) Summarised Accounts
1996-97 (2nd report 1998-99) ....HC 102, 1998-99

How the Utility Regulators are Addressing the Year 2000
Problem in the Utilities (13th report 1998-99)............... HC 449, 1998-99

The Millennium Threat (36th report 1998-99)...........…..........HC 517, 1998-99

Appendix 3: High level processes

Sector	Name	Responsible Body	Independent Assessor
Electricity	Provide Electricity	Office of Gas and Electricity Markets	Merz & McClellan
Gas	Provide Gas	Office of Gas and Electricity Markets	WS Atkins
Fuel Supplies	Supply Transport Fuel	Department of Trade and Industry	WS Atkins
	Supply Coal	Department of Trade and Industry	Aon Risk Services
	Supply Nuclear Fuel	Department of Trade and Industry	NII
	Provide Oil	Department of Trade and Industry	WS Atkins
Telecommunications	Provide Telecommunications	Office of Telecommunications	WS Atkins
Water and Sewage	Treat Dirty Water	Office of Water Services, Scottish Executive	Montgomery Watson; Halcrow
	Supply Clean Water	Office of Water Services, Scottish Executive	Montgomery Watson; Halcrow
Financial Services	Transmit Monies	Financial Services Authority, Bank of England	Financial Services Authority/Bank of England
	Trading Markets	Financial Services Authority	Financial Services Authority
	Provide Insurance	Financial Services Authority	Financial Services Authority
	Invest and Borrow Money	Financial Services Authority	Financial Services Authority
Essential Food and Groceries	Supply Goods	Essential Foods and Groceries Steering Group	PA Consulting
	Produce Food	Essential Foods and Groceries Steering Group	PA Consulting
	Process Food	Essential Foods and Groceries Steering Group	PA Consulting
	Distribute Food	Essential Foods and Groceries Steering Group	PA Consulting
	Sell to Customer	Essential Foods and Groceries Steering Group	PA Consulting
Rail Transport	Transport People and Goods by Rail	Office of the Rail Regulator, Her Majesty's Rail Inspectorate	WS Atkins
	Provide Rail Infrastructure	Office of the Rail Regulator, Her Majesty's Rail Inspectorate	WS Atkins
	Transport People by Underground	Government Office for London, Scottish Executive	Audit Commission
	Provide Cross-channel Rail Services	Intergovernmental Commission	Safety Commission
	Maintain Channel Rail Infrastructure	Intergovernmental Commission	Safety Commission
Air Transport	Transport People and Goods by Air	Civil Aviation Authority	Atomic Energy Authority Technologies Limited
	Provide Air Infrastructure	Civil Aviation Authority	Atomic Energy Authority Technologies Limited
Road Transport, Local Government	Provide Road Infrastructure	Department of Environment, Transport and Regions, Scottish Executive, National Assembly for Wales, Government Offices	Peer bodies, WS Atkins, Audit Commission, Accounts Commission for Scotland
Sea Transport	Transport People and Goods by Sea	Department of Environment, Transport and Regions , Maritime and Coastguard Agency, Scottish Executive	Maritime and Coastguard Agency
	Provide Sea Infrastructure	Department of Environment, Transport and Regions	Department of Environment, Transport and Regions, and to be appointed
Hospitals and Healthcare	Provide Healthcare Services	National Health Service Executive, National Health Service in Scotland, National Assembly for Wales	NHS Executive, Scottish NHS Executive, Audit Commission
	Provide Emergency Ambulance Service	National Health Service Executive, National Health Service in Scotland, National Assembly for Wales	NHS Executive, Scottish NHS Executive, Audit Commission
Fire Services	Provide Fire and Rescue Service	Home Office, Scottish Executive	HM Inspectorate of Fire Services, Scottish Office
Police	Police Emergencies	Home Office, Scottish Executive, British Railways Board (for British Transport Police)	Her Majesty's Inspector of Constabulary, HM Inspector of Constabulary Scotland
	Deal with Offences and Incidents	Home Office, Scottish Executive, British Railways Board (for British Transport Police)	Her Majesty's Inspector of Constabulary, HM Inspector of Constabulary Scotland
	Maintain Public Order	Home Office, Scottish Executive, British Railways Board (for British Transport Police)	Her Majesty's Inspector of Constabulary, HM Inspector of Constabulary Scotland
	Provide Policing Services	Home Office, Scottish Executive, British Railways Board (for British Transport Police)	Her Majesty's Inspector of Constabulary, HM Inspector of Constabulary Scotland
Broadcasting	Broadcast Information (BBC and radio only)	British Broadcasting Corporation Board of Governors, Radio Authority	KPMG & another to be appointed
Local Government	Co-ordinate Emergency Response	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
	Provide Housing	Government Offices, National Assembly for Wales, Scottish Executive, Housing Corporation, Scottish Homes	Audit Commission, Housing Corporation, Accounts Commission for Scotland
	Educate People	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
	Manage Sanitation and Waste Disposal	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
	Register Births, Deaths and Marriages	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
	Manage Death	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
	Maintain Public Health	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
	Provide Community and Nursing Care	National Health Service Executive, National Health Service in Scotland, National Assembly for Wales	Audit Commission, NHS Executive, Accounts Commission for Scotland
	Provide Social Services	Government Offices, National Assembly for Wales, Scottish Executive	Audit Commission, Accounts Commission for Scotland
Sea Rescue	Provide Sea Rescue Service	Department of Environment, Transport and Regions	Admiral Management Services
Weather Forecasting	Provide Weather Information	The Meteorological Office	National Audit Office
Post and Parcels	Distribute Letters	Department of Trade and Industry (Posts)	Impact
	Distribute Parcels	Department of Trade and Industry (Posts)	Impact
Welfare Payments	Pay Welfare	Department of Social Security	Impact
	Operate Post Office Counters	Department of Trade and Industry (Posts)	Impact
Flood Defence	Maintain Flood Defence	Ministry of Agriculture Fisheries and Food, National Assembly for Wales, Scottish Executive	Kennedy and Donkin, KPMG
Criminal Justice	Secure Prisoners	Home Office, Scottish Executive	DBi Associates (England and Wales)
	Run Court System	Lord Chancellor's Department, Scottish Executive	Yale Consulting
	Provide Post-sentence Support and Supervision	Home Office, Scottish Executive	HM Inspectorate of Probation (England and Wales)
Tax Collection	Collect Revenue	HM Treasury	Impact
Bus Transport	Transport People by Bus	Department of Environment, Transport and Regions	WS Atkins
Newspapers	Supply Newspapers	Department of Trade and Industry	WS Atkins

Appendix 4: UK National Infrastructure - Independent assessment by sector

Sector	Initial Results - January 1999	Position at 21 April 1999	Position at 12 July 1999	Position at 21 October 1999	Comments
Electricity	46% / 52% / 2%	71% / 29%	95% / 5%	100%	
Gas					
● Transmission	85% / 15%	95% / 5%	99% / 1%	100%	
● Prepayment meters	75% / 25%	80% / 20%	84% / 16%	100%	
● Shipping/ Suppliers	100%	7% / 64% / 7% / 22%	90% / 10%	99.7% / 0.3%	
Fuel Supplies					
● Offshore oil and Gas	100%	52% / 48%	97% / 3%	100%	
● Supply of fuel oils	100%	60% / 40%	82% / 18%	100%	
● Supply of coal (domestic)	100%	90% / 10%	95% / 5%	100%	
● Supply of nuclear fuel	100%	100%	100%	100%	
Telecommuni- cations	100%	90% / 10%	100%	100%	
Water and Sewage	100%	100%	100%	100%	
Financial Services					
● Payments clearing system	Not available	100%	100%	100%	*The results prior to 21 October 1999 were to a different set of colour codes used by the Financial Services Authority. For the October results the Action 2000 traffic light codes were used.
● Supply of cash	Not available	100%	100%	100%	
● Credit/Debit/ ATM Card Machines	Not available	100%	100%	100%	
● Regulated firms* - high impact bodies	93% / 7%	99% / 1%	98% / 2%	98% / 2%	100% blue projected 12 November 1999.
- medium impact bodies	85% / 15%	86% / 10% / 4%			continued...

Sector	Initial Results - January 1999	Position at 21 April 1999	Position at 12 July 1999	Position at 21 October 1999	Comments
Essential Food and Groceries	Not Available				
● Overall		● (orange)			
● Internal compliance			● (blue)	100%	
● Business continuity planning			● (orange)	100%	
● Top 12 retailers		● (blue)			
● Top 20 manufacturers		● (blue)	91% / 9%	100%	
● Next 10 retailers		● (orange)			
● Next 50 manufacturers		● (orange)			
Rail Transport	Not Available				Also Glasgow underground, London Docklands, Midlands, Metro, South Yorkshire Supertram, Tyne and Wear Metro all 100% blue. Manchester Metro (ALTRAM) not yet independently assessed.
● Business and operational systems		● (orange)	70% / 30%	100%	
● National rail safety systems		● (blue)	100%	100%	
● London Underground		● (orange)	75% / 25%	100%	
● Channel Tunnel		● (orange)	100%	109%	
Air Transport	Not Available				UK processes only. Scottish Island Services (Loganair) independent assessment underway.
● National Air Traffic Control Services		● (blue)	100%	100%	
● UK Airports		Not Available	100%	100%	
● UK Airlines		Not Available	87% / 13%	100%	
Road Transport	Not Available				
● Road traffic control equipment		98% / 2%	100%	100%	
● Motorways and trunk roads (England and Wales)		● (orange)	100% / ● (orange)	100%	
● Motorways and trunk roads (Scotland)		100% (outline)	67% / 33%	100%	

Sector	Initial Results - January 1999	Position at 21 April 1999	Position at 12 July 1999	Position at 21 October 1999	Comments
Sea Transport	Not Available				Scottish Island Services (CALMAC) 98% blue, 2% amber. 100% blue projected by 22 October 1999.
● Shipping		(amber)	55% (blue), 45% (amber)	100% (blue)	
● Ports		(amber)	85% (blue), 15% (amber)	100% (blue)	
Hospitals and Healthcare	Not Available				
● England		91% (amber), 9% (red)	4% (blue), 96% (amber)	100% (blue)	
● Wales		94% (amber), 6% (red)	100% (amber)	100% (blue)	
● Scotland		100% (amber)	100% (amber)	100% (blue)	
Fire and Rescue Services	Not Available				
● England and Wales		38% (blue), 38% (amber), 2% (red), 22% (white)	64% (blue), 36% (amber)	100% (blue)	
● Scotland		12% (blue), 63% (amber), 25% (white)	25% (blue), 75% (amber)	100% (blue)	
Police	Not Available				
● England and Wales		39% (amber), 9% (red), 52% (white)	2% (blue), 98% (amber)	100% (blue)	
● Scotland			100% (amber)	100% (blue)	
Broadcasting	Not Available				
● BBC		50% (blue), 50% (amber)	70% (blue), 30% (amber)	100% (blue)	
● Independent radio		Not Available	48% (blue), 3% (amber), 49% (white)	100% (blue)	
Local Government	Not Available	Not Available			
● England			6% (blue), 92% (amber), 2% (red)	100% (blue)	
● Wales			6% (blue), 93% (amber), 1% (red)	100% (blue)	
● Scotland			88% (amber), 12% (red)	100% (blue)	
Sea Rescue	Not Available	Not Available	100% (blue)	100% (blue)	
Weather Forecasting	Not Available	Not Available	86% (blue), 14% (amber)	100% (blue)	
Posts and Parcels	Not Available	Not Available	100% (blue)	100% (blue)	
Welfare Payments	Not Available	Not Available	100% (blue)	100% (blue)	

Sector	Initial Results - January 1999	Position at 21 April 1999	Position at 12 July 1999	Position at 21 October 1999	Comments
Flood Defence	Not Available	Not Available			
● England and Wales			95% 5%	100%	
● Scotland			50% 50%	100%	
Criminal Justice (England and Wales)	Not Available	Not Available			
● Crown Prosecution Service			100%	100%	
● Magistrates court			53% 47%	100%	
● Crown Courts			77% 23%	100%	
● Probation Services			36% 64%	100%	
● Prison Service and Prisons			30% 70%	100%	
Criminal Justice (Scotland)					
● Prison Service			4% 78% 18%	100%	
Tax Collection	Not Available	Not Available			
● Income and Corporation Tax			⬤	100%	
● VAT and Hydrocarbon Oil Duty			⬤	100%	
Bus Transport	Not Available	Not Available	75% 25%	100%	
Newspaper Publishing and Distribution	Not Available	Not Available	71% 29%	100%	

Appendix 5: Departments and Agencies making returns

Department	Agency(ies)	Department	Agency(ies)
Attorney General's Office (no return from centre)	Crown Prosecution Service	HM Treasury	Debt Management Office
	Serious Fraud Office	Home Office	Fire Service College
	Treasury Solicitor's Department		Prison Service
Cabinet Office	Buying Agency		UK Passport Agency
	Central Computer and Telecommunications Agency	Inland Revenue	Valuation Office
	Central Office of Information	Intervention Board	
	Civil Service College	Lord Advocate's Department (no return from centre)	Crown Office for Scotland
	Government Car Dispatch Agency	Lord Chancellor's Department	
	Property Advisers to the Civil Estate	Ministry of Agriculture Fisheries and Food	
Department for Culture Media and Sport		Ministry of Defence	Army
Department for Education and Employment	Employment Service Agency		Defence Evaluation and Research Agency
Department for International Development			Meteorological Office
Department of Environment, Transport and Regions	Driving and Vehicle Licensing Agency		Defence Procurement Agency
	Driving Standards Agency		Royal Air Force
	Highways Agency		Royal Navy
	Maritime and Coastguard Agency	National Insurance Contributions Office	United Kingdom Hydrographic Office
	Planning Inspectorate	National Savings	
	Queen Elizabeth II Conference Centre	Office for National Statistics	
	Rent Officer Service Agency	Ordnance Survey	
	Vehicle Certification Agency	Public Record Office	
	Vehicle Inspectorate	Royal Mint	
Department of Health (including Medical Devices Agency)	Medicines Control Agency	Scottish Executive	Scottish Agricultural Science Agency
	NHS Estates		Fisheries Research Services
	NHS Pensions Agency		National Archives of Scotland
Department of Social Security			Scottish Prison Service
Department of Trade and Industry	Companies House		Registers of Scotland
	Employment Tribunals Service		Student Awards Agency for Scotland
	Insolvency Service		Scottish Courts Service
	National Weights and Measures Laboratory		Scottish Fisheries Protection Agency
	Patent Office		Scottish Public Pensions Agency
	Radiocommunications Agency		General Registy Office
Export Credits and Guarantees Department	East Midlands		Historic Scotland
Foreign and Commonwealth Office	Eastern	National Assembly for Wales	Scottish Pensions Agency
Forestry Commission	IT (Central)		
Government Offices for the Regions	London		
	North East		
	North West		
	South East		
	South West		
	West Midlands		
	Yorkshire		
HM Customs and Excise			
HM Land Registry			

Appendix 6: Example of a country statement – France

Millennium bug: France

The following information has been collated by the British Embassy, Paris on the basis of information currently available locally. No guarantee is given as to its accuracy and no liability can be accepted in respect of any actions taken, or omitted to be taken, on the basis of the following information.

General

The French Government's Millennium Bug Task Force (Mission Passage Informatique a l'An 2000 - the "Mission") was established in February 1998 under the leadership of Gerard Thery. The Mission has around 15 members, the majority of whom are senior civil servants with a technical or engineering background.

In November 1998, Gerard Thery submitted a report to Dominique Strauss-Kahn, Finance, Economics and Industry Minister, and Christian Pierret, junior Industry Minister, analysing the current state of preparedness of key players, the actions already undertaken by the Mission and proposals for further measures.

The report contained two major conclusions:

■ some companies and government agencies had undertaken large-scale adaptation programmes which would prepare them well for the changeover (although this work had not been given substantial publicity);

■ in contrast, the status of SMEs deserved special attention and a sustained effort to raise their awareness of the problem.

Additional information about the Mission and its activities may be found, in both English and French, on its web site at www.an2000.gouv.fr).

Public authorities

The French Prime Minister Lionel Jospin issued a circular on 5 November 1998 to the members of his Government and to all Prefects (the local representatives of the State in each of the 100 or so Departéments) concerning measures to be taken by

public authorities to tackle the millennium bug. (published in the Journal Officiel No 258 of 6 November 1998). The circular underlined the importance of the issue, laid down the top priorities and set out the measures to be taken by the various arms of Government, both centrally and within individual Departments. It emphasised the need to ensure no disruption to essential services (notably energy, telecommunications, water, transport, health services and emergency services) and to guarantee the safety of industrial establishments, in particular nuclear facilities, and of other public buildings. Each Ministry has now appointed a senior official and has drawn up departmental action plans and contingency measures. These documents are available on the Internet (in order to access the action plans of individual ministries use the French Government's centralinternet directory at www.admifrance.gouv.fr). At local level, the Prefects in individual Departéments have been given the responsibility for co-ordinating action taken to combat the bug and spreading awareness in both the public and private sectors.

Large firms

Cigref (Club informatique des grandes entreprises francaises), an association bringing together the IT managers of France's largest public and private sector companies (EDF, SNCF, Elf Aquitaine, Peugeot, Aerospatiale, Rhone-Poulenc...) has played an important role in raising awareness of the bug among its members and planning strategies to combat it.

Cigref produced a major analysis of the problem, entitled Operation An 2000, in September 1998. It concluded that almost all large companies had put in hand an extensive programme to validate and, where necessary, modify their IT systems. In most cases, they had begun their preparations in 1996, if not before. Cigref noted, however, that problems could still arise and that the risk of malfunctions also resulted from external factors e.g. contact with suppliers or public services. Key members of Cigref including EDF, La Poste, France Telecom and Thomson-CSF have agreed to make their internal Y2K planning documents available on the Internet in order to assist other companies in their preparations (for further details, consult the Cigref web site at www.cigref2000.fr).

SMEs

The lack of awareness of the Y2K problem among SMEs continues to be a major concern for the Mission. The latest survey of 1800 heads of SMEs (0-199 employees; all sectors; fieldwork carried out in June 1999) showed an increase in the number of SMEs which have taken steps to adapt their electronic systems (1-199 employees: 56% - up from 52% in March; sole traders: 28% - up from 22% in March). Over 90% of companies with ten or more employees are now confident

that they will be ready before the end of the year. However, a substantial number of the very smallest companies still envisage taking no action (66% of sole traders, 37% of firms with 1-9 employees).

The Mission has already carried out a range of activities aimed at heightening awareness of the bug including mailshots to SMEs (800,000 in July 1998 and 2.2 million in December 1998), radio advertising and commissioning of the national benchmarking survey. Dominique Strauss-Kahn announced at the third meeting of the National Year 2000 Committee on 6 May that he was stepping up the publicity campaign: TV advertising, freephone number, eight roadshows visiting 100 French towns. The overall media budget for the French Y2K campaign (end 1997 to end 1999) is expected to work out at over 100 million francs (about £10 million).

Individual sectors

(i) Energy

Eléctricité de France (EDF), the state-owned company which runs the country's nuclear power stations as well as supplying and distributing electricity, conducted a full-scale test at its Civaux nuclear power station at the end of February 1999. The test was conducted by running the controls forward to three critical dates: 9 September 1999, 31 December 1999 and 29 February 2000; no malfunctions were detected. EDF has stated that those IT systems on which the smooth operation of the electricity network depend are Y2K compliant. It believes that the possibility of a general breakdown in electricity supply due to the millennium bug can be excluded (further details of the test and of EDF's millennium bug strategy can be found on the company's web site: www.edf.fr).

The French nuclear safety authority has stated that it will not hesitate to shut down any nuclear power station where it believes that there is a safety risk linked to the bug. The four research reactors operated by the Commissariat á l'Energie Atomique will be shut down over the New Year period, as will all Cogema (nuclear fuel reprocessing) plants with the exception of its uranium enrichment facility, Eurodif.

Gaz de France has received assurances from its overseas gas suppliers, notably The Netherlands, Norway, Algeria and Russia, concerning Y2K conformity. The gas supply infrastructure in France has a relatively low level of automation. Nevertheless, a crisis plan is being drawn up to enable manual operation if IT systems should fail.

(ii) Water

Water supply and sewerage services are the responsibility of individual "communes" (the lowest level of local administration in France). In most cases, a concession is granted for the provision of these services.

Water supply and purification will also be addressed at local level by the Action Plans to be drawn up by the Prefect in each Departement.

(iii) Telecommunications

Although the telecomms sector has been opened up to competition, France Telecom remains the dominant operator. The level of preparedness of France Telecom is therefore likely to have a very significant impact on the ability of the sector as a whole to continue functioning normally into the Year 2000.

France Telecom has been working since 1996 to prevent operational problems likely to affect its computer and technical systems during the changeover. 500 people and around 1 billion francs (£100 million) are being devoted to the task. The inventory of France Telecom's different IT systems (over 1500) was completed in June 1998. It was found that adaptation or replacement would be necessary for around 25% of them. The adaptation of its general data processing applications was completed by the end of 1998.

France Telecom has now confirmed that its entire system is ready for the Year 2000 transition. Furthermore, the company will have 150 people on duty on the night of 31 December/1 January to carry out tests on IT equipment and 300 people will be working on 2 January. Further teams will be in place to monitor the situation over the period 28/29 February.

(iv) Transport

(a) Air

The Direction Generale de l'Aviation Civile (DGAC), part of the Ministry of Infrastructure, Transport and Housing, has taken the lead in ensuring the safety of air transport and continuity of service during the millennium changeover. It has been actively pursuing this task since 1997.

The DGAC has drawn up a plan for handling the bug in each of three key areas: air traffic control, air-worthiness and airport safety. For air traffic control, following the completion of an inventory of IT systems, the second half of 1998 was devoted

to modification and validation of individual systems. The deployment of modified systems began in the middle of January. According to the DGAC, the majority of mission critical systems had been passed as Y2K compliant by end June 1999, thus meeting the objective set out in the organisation's action plan. A table giving a detailed read-out (in English and French) of the preparedness of each critical function can be found on the DGAC website (www.dgac.fr).

For air-worthiness, the DGAC is working both with French airlines and French constructors. The DGAC is responsible for verifying that, where a constructor has asked for modifications to be made, this work has been carried out. If not, the DGAC may revoke the air-worthiness certificate of the aircraft concerned. Reports were submitted to the DGAC in the first quarter of 1999 by constructors and airlines on their state of preparedness. According to the DGAC no Y2K-related risks have been identified by the constructors which could endanger the aircrafts' handling.

The DGAC has also been overseeing the preparations of French carriers and has recently published a progress report in line with ICAO guidelines. All French operators are continuing to carry out a programme of tests and/or modifications to ensure that the on-board equipment is Y2K compliant. 57% of French operators have successfully completed compliance programmes for their ground systems (e.g. flight preparation, maintenance, crew-rostering); for the remainder, work is continuing.

The DGAC has also been directly involved in verifying the Y2K compatibility of airport safety systems (e.g. equipment for detecting weapons and explosives) and has reported that this is proceeding satisfactorily (details for individual screening devices can be found on the DGAC website).

Air France conducted an impact analysis of its computer systems early in 1997 and appointed a specific unit to tackle the problem in September of that year. The Year 2000 Programme Manager submits reports to the Air France's general management every two months. In the last financial year around 120 person-years were devoted to the issue. The company's objective is to ensure that all in-house business-critical systems are fully compliant by end June 1999.

The DGAC has also been overseeing the preparation of airports, notably Aeroports de Paris (the company operating Orly and Charles de Gaulle airports). The chairman of Aeroports de Paris stated in February that 70% of its systems

(excluding air traffic control) were compliant, 15% were awaiting adaptation, 12% had still to be analysed and 3% had revealed serious problems (e.g. the supplier could not be traced or there was no ready fix available).

(b) Road transport

The Ministry of Infrastructure, Transport and Housing has carried out an inventory of the different organisations and IT systems of relevance to the millennium bug problem. These systems have been prioritised (e.g. roadside emergency phones and traffic light management systems are in the highest priority "crucial" category). The various organisations responsible for road traffic matters have been contacted by the Ministry. Particular attention is being given to potential problems with computer-controlled traffic management systems governing traffic flows in large urban areas.

(c) Water transport

For maritime transport, priority has been given to the verification of signalling, surveillance and rescue systems. For inland waterways, the automatic operation of locks is being verified under the auspices of the relevant public body, Voies Navigables de France. The Ministry wrote to French port operators in December 1998 with a questionnaire on their millennium compliance and a parallel questionnaire was sent to French ship owners in February 1999.

(d) Channel Tunnel

Work is in progress to ensure that the Channel Tunnel is Y2K compliant. This work is being carried out under the aegis of the bi-national Franco-British Channel Tunnel Safety Authority and Inter-Governmental Commission. Eurotunnel has announced that it will not be running any commercial trains through the tunnel on the night of 31 December 1999.

(v) Financial sector

The Mission's November 1998 report notes that planning for the bug started very early in this sector. It concludes that, on the whole, it appears that all components of the Paris financial market are well advanced in their programmes to achieve Y2K compliance. The report notes that these programmes have benefited enormously from the experience of the changeover to the single currency which shares many technical features with the millennium transition.

The Commission Bancaire (banking supervisory body) believes that large banks are well prepared with around 20% currently running ahead of schedule. The situation of other banks is also broadly satisfactory. In August 1999 successful tests of the interbank payment systems were undertaken. The Bourse de Paris (stock exchange) has run a series of three tests, the first lasting from 27 May until 3 June, simulating 28/29 February 2000 as well as the New Year period. Financial markets will be closed on 31 December and reopen on 3 January.

(vi) Health

The Direction des Hopitaux (part of the Ministry of Employment and Solidarity) has taken a number of steps to ensure that medical establishments in France have addressed the millennium bug problem. A ministerial circular was issued in October 1997 and a lead official was designated in May 1998 with four main tasks:

- to provide technical assistance to private and public sector establishments;

- to ensure effective coordination and experience-sharing;

- to raise awareness among suppliers;

- to monitor the progress made by individual hospitals.

Among the measures undertaken have been the establishment of three pilot hospitals (Amiens, Montfavet and Saint Nazaire) as test-beds for methodological studies, the production of a practical guide to coping with the bug and the creation of a network of teaching hospitals to pool and disseminate experience.

Appendix 7: List of Foreign and Commonwealth Office country statements

Angola	Anguilla	Antigua & Barbuda
Argentina	Australia	Austria
Azerbaijan	Bahamas	Bahrain
Bangladesh	Barbados	Belarus
Belgium	Belize	Brazil
British Virgin Islands	Brunei	Bulgaria
Burundi	Cambodia	Cameroon
Canada	Cayman Islands	Central African Republic
Chad	China	Colombia
Commonwealth of Dominica	Costa Rica	Cuba
Cyprus	Czech Republic	Denmark
Dominican Republic	Egypt	El Salvador
Estonia	Equatorial Guinea	Falkland Islands
Finland	France	Gabon
Georgia	Germany	Gibraltar
Greece	Grenada	Guyana
Haïti	Honduras	Hong Kong
Iceland	India	Indonesia
Ireland	Israel	Italy
Jamaica	Japan	Jerusalem
Kazakhstan	Kenya	Korea
Kuwait	Kyrgyz Republic	Latvia
Lebanon	Lithuania	Luxembourg
Macedonia	Madagascar	Malawi
Malaysia	Malta	Maldives
Mauritius	Mexico	Mongolia
Morocco	Mozambique	Namibia
Nepal	Netherlands	New Zealand
Nicaragua	Nigeria	Norway
Oman	Pakistan	Panama
Peru	Philippines	Poland
Portugal	Qatar	Romania
Russia	Rwanda	Saudi Arabia
Seychelles	Singapore	Slovakia
Slovenia	Solomon Islands	South Africa
Spain	Sri Lanka	St Kitts & Nevis
St Lucia	St Vincent & The Grenadines	Swaziland
Sweden	Switzerland	Syria
Taiwan	Tanzania	Thailand
Tonga	Trinidad & Tobago	Tunisia
Turkey	Uganda	Ukraine
United Arab Emirates	Uruguay	USA
Venezuela	Vietnam	Yemen
Zambia	Zimbabwe	(list as at 26 October)

Appendix 8: Year 2000 Internet web sites around the world

Individual

Algeria
www.y2k.net.dz

Argentina
www.sfp.gov.ar/2000/2000 (Spanish)

Armenia
http://y2k.sci.am

Australia
www.y2k.gov.au , www.dcita.gov.au and www.ogit.gov.au/year2000

Austria
www.wifi.at/tub/2000/ and www.austria.gv.at/e/jahr2000e/year2000.htm

Bangladesh
www.bccbd.org

Belarus
http://y2k.bas-net.by

Belgium
www.Y2000.fgov.be and www.belgacom.be

Benin
http://www.a2mben.bj

Bolivia:
http://www.sisteco-bo.com/bolgob-y2k

Bosnia-Herzegovina
http://www.mvp.gov.ba/y2k

Brazil
www.a2000.gov.br

Brunei
www.brunet.bn/gov/y2k

Bulgaria
www.y2k.govn.bg/y2k

Canada
www.info2000.gc.ca and http://strategis.ic.gc.ca and www.parl.gc.ca

Chile
www.a2000.cl

Colombia
www.2000.gov.co

Costa Rica
www.micit.go.cr

Croatia
www.mzt.hr/mzt/hrv/informatika/2000

Cuba
http://www.islagrande.cu/eventos/info2000/homenc

Denmark
www.fsk.dk and www.2000parat.dk

Dominican Rep.
www.bancentral.gov.do (Spanish) and http://www.comision2000.gov.do

Ecuador
www.superban.gov.ec/doc/impacto and www.ec.gov.net/y2k

Egypt
www.sis.gov.eg/online/y2k/html/

El Salvador
http://superval.gob.sv (Spanish)

Estonia
http://www.riik.ee/2000

Ethiopia
www.telecom.net.et/y2k

EU
www.ispo.cec.be/y2keuro/year2000

Finland
www.vn.fi/vm/suomi/muuta/vhtt/index.htm

France
www.an2000.gouv.fr and www.urgence2000.gouv.fr (English) see also
www.gdf.fr/anglais and www.cigref2000.com

Georgia
http://www.y2k-pmu.kheta.ge

Germany
www.iid.de/jahr2000 (English) and www.bundesbank.de/index_e (English)

Ghana
www.y2kghana.gov.gh

Greece
Via EU website - see above or www.year2000.gr

Guatemala
http://www.dia2000.org.gt

Holland
www.mp2000.nl and see also www.FHI.nl/2000/eng and www.energie2000.nl

Honduras
http://www.y2k.hondunet.net/

Hong Kong
www.year2000.gov.hk

Hungary
www.itb.hu/fejlesztesek/2000 and http://www.y2k.gov.hu

India
www.y2k.gov.in

Indonesia
www.y2k.or.id

Iran
http://www.y2k.hci.or.ir

Irish Republic
www.irlgov.ie www.aerlingus.ie and www.esb.ie

Israel
www.mof.gov.il/2000 (Hebrew)

Italy
www.tesoro.it and try www.aipa.it/attivita/anno2000 see also Italy's report to the EU
(address listed above)

Japan
www.zenginkyo.or.jp/en and www.kantei.go.jp/foreign/y2k (English)

Jordan
http://www.y2k.gov.jo

Kenya
www.y2kkenya.go.ke

Kyrgyz Republic
http://www.y2k.kg

Luxembourg
www.crpht.lg/a2000, www.y2k.lu, http://www.crpht.lu/an2000/ and
www.spiral.lu/lil/projects/an2000

Macau
www.cpttm.org.mo/y2k/english/

Macedonia
http://www.y2k.gov.mk

Malaysia
www.y2k.gov.my

Mauritius
http://ncb.intnet.mu/y2k

Mexico
http://pdi.inegi.gob.mx/2000 and see www.secodam.gob.mx/proy2000

Moldova
http://mci.gov.md/year2000

Morocco
www.septi.gov.ma

New Zealand
www.y2k.govt.nz

Niger
http://www.delgi.ne/an2000/

Norway
www.aksjon2000.org see also http://odin.dep.no/aad/publ/aar2000 (English)

Pakistan
www.pcb.gov.pk

Panama
http://www.y2k.gob.pa

Peru
www.inei.gob.pe/pia2000

Philippines
www.y2k.gov.ph

Poland
http://www.dli.mswia.gov.pl (Polish)

Portugal
http://ano2000.mct.pt, www.eunet.pt/ano2000 and
www.iapmei.pt/idex/informacao/ano2000

Russia
www.ptti.gov.ru (Russian) and www.2000.ru

Senegal
www.primature.sn/an2000

Singapore
www.ncb.gov.sg/ncb/yr2000

Slovakia
www.infostat.sk/y2k/index.html and www.forum2000.sk (Both in Slovak only)

South Africa
www.y2k.org.za see also www.telkom.co.za

South America
www.foroy2kamericadelsur.org

South Korea
http://y2000.nca.or.kr

Spain
www.map.es/csi/2000.htm and www.endesa.es/2000

Sri Lanka
www.lk/2yk1.html

Sweden
www.2000-Delegationen.gov.se (has English version)

Switzerland
www.millennium.ch

Taiwan
www.dgbasey.gov.tw/dc2000 and http://www.year2000.gov.tw/

Thailand
www.y2k.nectec.or.th

Tunisia
www.an2000.tn

Turkey
http://y2000.dpt.gov.tr (Turkish)

UAE
www.gulfnetec.com/Y2K/Y2Khome.htm

Uganda
www.y2kuganda.go.ug

Ukraine
http://www.ipi.kiev.ua

Uruguay
www.opp.qub.uy/y2k and http://www.opp.gub.uy/y2k

USA
www.y2k.gov see also www.fcc.gov/year2000 and www.nrc.gov,

www.sba.gov/y2k, www.fda.gov/cdrh/yr2000

Venezuela
www.platino.gov.ve/ano2000

General

United Nations – www.un.org/members/year2000

World Bank – www.worldbank.org/y2k and www.iycc.org/countryfact.htm

The Information Systems Audit and Control Association and Foundation – www.isaca.org

European Commission – www.ispo.cec.be/y2keuro

International Telecommunications Union – www.itu.int/y2k