Year 2000 (Y2K) compliance – origins, obstacles and opportunities

A.S.C. Hooper
C/o: Department of Information Systems, University of Cape Town, Rondebosch, 7700 Republic of South Africa
Colchest@iafrica.com

This article considers the problems posed by the software and hardware components of Year 2000 compliance. Different perspectives are explored to obtain an understanding of the technical as well as business decisions that need to be faced as the deadline approaches. Particular attention is paid to the standards being set for Y2K compliance. Processes for achieving compliance are summarised and reference is made to specific mechanisms and how to obtain details. To concentrate on the more positive business aspects and opportunities, ways in which the compliance process can be approached to enhance a company's business offering and competitiveness are explored. Suggestions are made as to who is responsible for addressing the risks and how to minimise them, bearing in mind the legal elements involved. Because of the large amount of uncertainty associated with the 'millennium bug' and its consequences, some attention is paid to what can be done to pick up the pieces after 1st January, 2000.

Hierdie artikel neem die probleem van die gereedheid van sagte- en hardeware komponente vir die jaar 2000 in oënskou. Verskillende perspektiewe word ondersoek om sodoende begrip te kry van die tegniese sowel as die besigheidsbesluite wat geneem moet word namate die sperdatum nader kom. Besondere aandag word gegee aan die standaarde wat gestel word vir Y2K-gereedheid. Prosesse vir gereedmaking word opgesom en verwysing word na spesifieke meganismes gemaak. In 'n poging om op meer positiewe besigheidsaspekte en geleenthede te konsentreer, word maniere ondersoek waarop die gereedheidsproses benader kan word om 'n maatskappy se mededingendheid te verbeter. Voorstelle word gemaak oor die aanpak van die probleme en hoe risiko's met inagneming van regsaspekte verminder kan word. Vanweë die grootskaalse onsekerheid oor die 'millennium-virus' en die gevolge daarvan, word aandag gegee aan die herstel van skade na 1 Januarie 2000.

Origins

It is important at the outset to have a clear understanding of what constitutes 'the millennium bug'. Without doubt this is the most extraordinary concatenation of circumstances imaginable, having its roots as far back as the dawn of human civilisation and mankind's attempts to measure and record time. Add to that a mixture of Renaissance science, Reformation religion and the politics of church and state. Then bring the mix right up to date with the need to conserve computer memory when programming in the 1960s and 1970s without any thought for the consequences when the millennium changed. Those consequences may be dire, and are expected to be of world-wide significance. They cannot be ignored by anyone, for very few people will be unaffected.

The origin of the problem is very readably explained by Murray and Murray (1996). It has its roots in mankind's attempts to measure time by astronomical observation. The original calculation of a year being 365.25 days led to leap years being decreed by Julius Caesar in 46 BC to resolve the mess which resulted from the Romans using a calendar based on 12 lunar cycles, or lunations. However, a leap year every four years was not sufficient to adjust to the difference between the 365.25 and the actual 365.242 days in each year. By 1582, the discrepancy had put the Julian calendar ten days out from the solar year. Pope Gregory XIII decreed dropping ten days immediately and changing the leap-year definition. The Gregorian Calendar allowed every fourth year to be a leap year, but 'any centesimal year (a year ending in two zeros, e.g. 1600, 1700, 1800) not evenly divisible by 400 would not be considered a leap year' (Murray & Murray 1996:5).

The Gregorian Calendar was adopted only gradually – some countries in 1582, others later. Britain and its colonies, (including pre-Revolutionary America), finally did so in 1752 by when the error was eleven days. (*Goal2000* 1996). Section II of the 'Act substituting the Gregorian for the Julian Calendar' [24 Geo. II cap. 23] enacts:

> 'That the several years of our Lord 1800, 1900, 2100, 2200, 2300, or any other hundredth year of our Lord, which shall happen in time to come, except only every four hundredth year of our Lord, whereof the year of our Lord 2000 shall be the first, shall not be esteemed or taken to be bissextile or leap years, but shall be taken to be common years, consisting of 365 days, and no more; and the years of our Lord 2000, 2400, 2800, and every four hundred year of our Lord, from the year of our Lord 2000 inclusive, and also all other years of our Lord, which by the present supputation are esteemed to be bissextile or leap years, shall for the future, and in all times to come, be esteemed and taken to be bissextile or leap years, consisting of 366 days, in the same sort or manner as is now used with respect to every fourth year of our Lord' (*Goal2000* 1997).

This then explains why the year 2000 is a leap year, but not why there is a problem with computers handling leap years, and specifically the leap year in 2000 AD.

The problem of programming practice whereby six-digit dates were used had its origin in the punched cards used in the first IBM 1401 computers introduced in 1959. The System 360 computers which replaced them, in the interests of compatibility, continued to use a six-digit date sequence. Then on November 1st 1968, the US Department of Commerce, National Bureau of Standards, issued *Federal Information Processing Standards Publication 4* (FIPS PUB4) which also specified the use of six-digit dates for all information exchange among federal agencies (Murray & Murray 1996:xiv).

The problem of a six-digit date field is that a computer cannot recognise that Monday January 3rd 2000 as it appears in a six-digit date form (01/03/00, or even 03/01/00) is a later date than October 10th 1999 (10/10/99).

> 'The essence of the crisis is that the world's application software cannot continue to function by using six-digit dates. Without extensive modification or complete rewriting, this software won't function even if provided with adequate dating data. The absolute time to failure depends on the nature of the computing tasks for any given computer user ... The certain deadline is Saturday, 1st January, 2000' (Murray & Murray 1996:xv.)

Gerner (1996) gives other reasons why the computer problem exists. These include

- Lack of date standards. With no standards to work to, management and IT staff were often left to choose whatever suited them.
- Computing resource constraints. Main memory, disk space and even punched card space was at a premium in the early days of computing. It made sense therefore, not to include any extra digits for years.
- Minimising user work load on keying. Time was saved on data capture by using the 'standard' two digits for years.
- Applications lasted longer than expected. A typical justification for using a date algorithm which would fail when processing dates outside the 20th Century was that the application wouldn't last outside that era anyway.
- Backwards compatibility. Every new application written is expected to maintain some form of compatibility with previous systems... The market has demanded backwards compatibility, basically because users have been reluctant to replace working applications with the latest models.
- Code reuse. Virtually all new applications have algorithms and even codes incorporated from previous systems. This speeds up development and results (usually) in more reliable systems.
- Historical data built up painstakingly over an organisation's history is considered a corporate asset. Successive applications are built on this asset on the basis of what may be faulty data.
- Procrastination. A significant proportion of MIS departments have been putting off dealing with the problem, usually in the hope that a solution will emerge in time.

Why then is the problem so extensive? Murray and Murray (1996:xv–xvi) identify just how many lines of programming code are required to be re-written to solve the problem and how long this would normally take in calendar years to accomplish. The Gartner Group estimates that an organisation will spend between US $1.00 and US $1.50 per line of code to analyse and correct the year 2000 problem. Translated this means that an organisation will spend twice the annual cost it spends on maintaining its applications, and that there is no sustainable benefit from such a large expenditure (Deloitte & Touche 1998a).

There are other such calculations, but the general conclusion remains the same – the task is either immense or impossible to accomplish in the time available. In addition, besides the problem of reprogramming, there is the problem of embedded chips which are not Year 2000 compliant. Identifying where they are and how to eliminate any deleterious effects greatly magnifies the complexity of the problem.

The net result is that there are millions of lines of program code embedded in computer applications software packages which are mission critical for innumerable functions in business and government all over the world. Because this problem may be found in millions of ageing software applications, the costs of fixing the 'year 2000 problem' appear likely to constitute the most expensive single problem in human history (Capers Jones 1997).

Just to complicate matters further, Peter de Jager expressed his concern that most IS people were 'unprepared or unconcerned' and identified the problem as follows:

> 'The task facing us is to identify and correct all the date data and check the integrity of all calculations involving the date information. We must correct the data residing in all data files or write code to handle the problem ... How do we identify the problem data and the associated calculations? We have few, if any, standards for labeling data used in date calculations. The only choice we have is to examine each line of code and make the necessary changes ...' (De Jager 1993)

If the problem is not fixed, then the errors in software associated with communications, finance, taxation, insurance, and even transportation can also lead to the most expensive litigation in human history. However, to propose a positive element, once the problem is fixed, enterprises will have a much better knowledge of their software portfolios and application structures than ever before. In addition, although there have been dire predictions of disaster in many enterprises, the millennium bug can be seen as an opportunity.

The purpose of this essay is to explore some of the threats, but to concentrate on the more positive business aspects and opportunities. It will look at the software and hardware elements of Y2K compliance and the problems associated with each. Different perspectives will be explored to obtain an understanding of the technical as well as business decisions that need to be faced as the deadline approaches.

Particular attention will be paid to the standards being set for Y2K compliance. It is intended that the essay will identify ways that the compliance process can be approached to enhance a company's business offering and competitiveness rather than just being seen as a non-productive expenditure of resources to avoid a potential problem of unknown proportions. Because of the large amount of uncertainty associated with the 'millennium bug' and its consequences, attention will be paid to what can be done to help businesses pick up the pieces after the 1st January, 2000.

The first requirement is to identify what criteria have been identified for Year 2000 compliance as these constitute a standard or definition towards which all further activity is directed.

Obstacles – standards for conformity

The British Standards Institution has produced the most widely accepted version of what constitutes Year 2000 Conformity. It reads as follows:

> 'Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the year 2000.
>
> In particular:
>
> Rule 1. No value for current date will cause any interruption in operation.
>
> Rule 2. Date-based functionality must behave consistently for dates prior to, during and after year 2000.
>
> Rule 3. In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.
>
> Rule 4. Year 2000 must be recognized as a leap year' (British Standards Institution 1997).

This rather cryptic statement is further amplified as follows:

> 'Problems can arise from some means of representing dates in computer equipment and products and from date-logic embedded in purchased goods or services, as the year 2000 approaches and during and after that year. As a result, equipment or products, including embedded control logic, may fail completely, malfunction or cause data to be corrupted.
>
> To avoid such problems, organisations must check, and modify if necessary, internally produced equipment and products and similarly check externally supplied equipment and products with their suppliers. The purpose of this document is to allow such checks to be made on a basis of common understanding.
>
> Where checks are made with external suppliers, care should be taken to distinguish between claims of conformity and the ability to demonstrate conformity'.

Various rules and notes are then given which are worth consulting in the original document.

The official Canadian definition is more explicit but tends to tautology. (See the Canadian government official web site: www.info2000.gc.ca). Other organisations, especially organisations such as the US Army and Navy, and those that are dependant on large contracts for the supply of electronic and other equipment, give their own definitions of compliance. A number of them, both South African and foreign, can be found at www.y2k.org.za, the web site of the South African National Year 2000 Decision Support Centre. The South African definition was published *inter alia* in the *Sunday times Business times* on 31st May 1998.

Obstacles – Y2K risks

The first risk is that there is no universal definition of Year 2000 'compliant', 'ready', 'capable' or 'compatible'. The actual meaning will have to be determined in law by the context of the statement. Two 'compliant' systems may be completely unable to exchange data involving dates after 12/31/1999. A 'ready' system may be unable to work in the Year 2000 without additional modification, but it's 'ready' for that modification. A good warranty should define these terms in language that a court could understand (Hassett 1997). However most organizations are being advised not to issue warranties or to make statements that indicate complete compliance because of the vulnerable situation in which such a statement might place them should they suffer from a 'knock-on effect' from lack of compliance by important business associates (Cromhout 1998).

The second side to the risk is that it is not confined to mainframe software or legacy systems, but includes embedded components in personal computers, process control systems as well as PABX and microprocessors. These are to be found in such varied equipment as

- Environmental control units
- Factory printing and packaging machinery
- Process control and monitoring equipment
- Security and access control systems
- Telephone exchanges
- Traffic lights
- Civilian and military avionics
- Lifts/elevators
- Power stations
- Hospitals (Delloitte & Touche 1998n, 1988o, 1998p).

The third side to the risk is that it contains legal, economic and socio-political consequences that are largely beyond the control of any single individual or organisation to rectify. This means that although an organisation may achieve compliance at great cost in time and money, that investment may be compromised by other business associations that it cannot anticipate or control.

Gregg Gordon, in an article in *Business times* quotes Dr Maarten Venter, group general manager, Business Systems Division, at Absa Bank, as saying that there are two important year 2000 issues – guarding against investing money in pure throwaway fixing (and recognising that) there are few large computer systems around the globe that are not in some way directly connected to many other systems.

> 'The ultimate risk lies not within our own systems, but in our ability to safeguard our core against the failure in other systems, putting the whole macro system at risk' (Gordon 1998).

A recent report by market-research firm Gartner Group indicates that while most large corporations have Year 2000 problem resolution well underway, small companies are less active in fixing their systems.

> 'More than half of corporations with 20,000 employees or more are likely to fix all Year 2000 bugs in time for the millennial turnover, but 88 percent of firms with fewer than 2,000 employees have not yet even started their Y2K conversion projects. Analyst Matthew Hotle says that there could be serious problems in the supply chain. One large automaker with a Year 2000 project underway relies on parts made by a small supplier that has not yet begun one, possibly causing its assembly line to come to a stop if the latter's computers crash. Gartner recommends that companies perform "triage" on their extranets and supplier networks to determine what if any Year 2000 efforts are underway at their business partners' sites' (Wilson 1997).

Business day reported on 18th March, 1998, that the Australian Stock Exchange has told its 1200 listed companies to 'disclose their plans for dealing with the millennium computer bomb by June 30 or face suspension of trading in their shares' (Millenium trading curbs threatened 1998). This requirement would appear to fit in with the need for businesses not to issue warranties declaring their compliance, but merely to indicate their understanding of the problem, and what their plans are for addressing it.

Business risks can therefore be summarized as being:

- Embarrassment due to failure of critical systems resulting in breach of contract, unavailability of services, loss of processing facilities, as well as loss of supplier, employee, investor and customer confidence.
- Loss of revenue from delayed banking, invoicing and collecting with consequent interest loss and uncollectable debts.
- Increased cost of business from loss of data and the associated recovery time, the cost of processing backlogs, legal costs associated with litigation and settlement, penalties for non-compliance with statutory or contractual requirements, and any additional public relations costs.
- Financial misstatement including incorrect data and loss of system integrity, incorrect valuations of assets, non-disclosure of contingent liabilities.
- Competitive disadvantage resulting in loss of business and customers.
- Legal liability from breach of contract or claims by stakeholders.
- Regulatory, statutory or contractual liability resulting from lack of provision of adequate services, Copyright legislation, Data Protection legislation, Public Accountability, Companies Act requirements, etc.
- Loss of public trust (Deloitte and Touche 1998c).

Throughout the world it is expected that a flood of law suits will be filed some time after the Year 2000. Hassett considers that a smaller number will begin to be filed when the 'problem' manifests itself in forward-looking systems, or if statutes of limitations are running out. The basis for these law suits will include breach of warranty or representation, fraud, and any number of actions under consumer protection laws. In addition, there may be suits against directors and officers for negligence in management (breach of the duty of care). Already there is a 'paper blizzard' underway, with enquiry letters and questionnaires being mass-mailed between customers, vendors, suppliers and distributors. In some cases, businesses may be legally required to provide an answer. In other cases, they may have no such obligation. The problem is that the enquiries, and the responses they generate, are of great legal significance (possible setting up legal liability) and should not be undertaken without legal consultation. (Hassett 1997).

Where does ownership lie? Clearly it is every businessman's responsibility to ensure that his systems are compliant, and that the systems of his immediate business partners, suppliers and customers are also compliant. Company directors have a duty to act with care and skill in the discharge of their duties. Section 247 of the Companies Act, No 61 of 1973, provides that a director cannot be indemnified against any liability towards his company which would normally result from his negligence or breach of duty. This provision is compounded by Section 13(1) of the Prescription Act, No 68 of 1969, so that a person who was a director during the period from 1996 to 2000 may face litigation whether or not the company is still in business after the latter date (Deloitte and Touche 1998g).

Auditors have special responsibilities and cannot simply ignore the problems of their clients. Not only do they need a proper understanding of the Year 2000 issues for their clients, they also need to address the risk associated with non-conformance and particularly when involved in the rectification process. Negative remarks about an organisation's Year 2000 compliance could have the auditors subject to litigation. Other unexpected and serious consequences for both clients and auditors could include customers changing their supplier, employees leaving the employ of a company and banks refusing or withdrawing credit facilities. To assist auditors with their task of assuring that compliance with Year 2000 compliance has been attained, a number of audit tools can be expected during the coming months (Deloitte and Touche 1998h).

In September 1997, Wall Street economist Dr Edward Yardeni claimed that there is a 35% chance that the year 2000 software problem will lead to a mild global recession in that year.

> 'Yardeni says the year 2000 problem is a serious threat to the global economy, and one that is not being paid the attention it is due. Companies depend on their computers for internal and external links, so

> any small failures will have a ripple effect, according to Yardeni. Yardeni's prediction is based on public documents from the Federal Reserve Bank, the IRS, European banking regulators and other sources rather than on original research' (Scheier 1997).

Investment advisors now believe that, if anything, the magnitude of the problem has been underestimated. Even companies that do not rely on information technology or that have resolved their internal year 2000 compliance requirements can still be severely crippled as a result of problems experienced by business partners, suppliers or customers. Deloitte and Touche estimate that 10% to 20% of all businesses will fail and cease operations completely. Another 20% will survive the change in millennium but with serious difficulties. As a result of the large number of companies experiencing difficulties from non-compliance, Stock Exchanges around the world are expected to experience corrections as surviving companies race ahead at the expense of those in difficulty. To prevent the investment community from becoming panicked they recommend that all listed companies obtain independent assessments of their Year 2000 compliance state. Even if a company is not completely compliant, its directors may choose to consider appropriate disclosure to calm the stakeholders and protect the company's ongoing viability (Deloitte and Touche 1998i).

Another side to the problem is that companies and public bodies are unable or unprepared to establish a database of those companies and their products that are (or are not) Year 2000 compliant for fear of litigation. Such litigation could be initiated by the company concerned or by customers who discover that the information in the database is incorrect.

Obstacles – finding the solution

Is there a 'silver bullet' solution being developed somewhere in the world which will finally resolve the problem?

Some companies are unveiling testing and inventory tools that may ease the identification of trouble spots. Others are hoping that bombarding people with information is the best remedy. Software developers are eager to redeem their stature and are rolling out new and promising tools. One example is Think 2000, from Thinking Tools Inc. that simulates scenarios to help IT managers and executives prioritize steps they need to take to decrease the business impact of potential year 2000 systems failures (McCright 1997) .

In a hard hitting article, Peter de Jager (1996) refutes the idea of there being any 'silver bullet' to solve the problem as being a 'search for the Holy Grail'. However he recognizes that tools can deliver a saving of 20–30% in helping to deal with the problem. (In an earlier article in 1993, he identified the value of object-oriented systems as providing some good news about the millennium bug, De Jager 1993.)

With increasing levels of uncertainty – and the only certainty is the inevitability of the approaching date – people throughout the world seek reassurance and guidance. Investors want to know that the problem is understood by management and that something is being done. Of prime importance is an understanding that the management level of project ownership is appropriate for the seriousness of the problem.

For management, the concern is wider. Primarily they need the reassurance that Y2K projects will be completed in time, that the outcome will be aligned to expectations and that national and international business can proceed without interruption. However, as the date approaches other concerns arise. How will employees react? Will credit facilities be available? What will happen to suppliers, markets, customers, transport, raw materials? What should the company be saying to customers, suppliers and shareholders? Should the company repair or replace its systems, and if so when? Each sector will have different concerns.

On a national level it is important that related industries are talking to one another and to this end governments throughout the world have developed National Year 2000 Decision Support Centres. In South Africa Deputy President, Thabo Mbeki, is charged with responsibility for its activities. This indicates the general perception that the problem is of such enormity that it demands attention at an appropriately high level. At best Decision Support Centres can help ensure that due attention and publicity is being given to the problem. They can also provide help desk facilities for those sectors that suddenly discover the likely consequences for themselves.

Whatever stakeholders want to hear, they need to understand the nature of the problem and realise that they too will have to share it in one way or the other. No one can be certain what will happen as the new millennium rolls in. The problem is so big that everyone will have to work on it. Very few organisations will be 100% compliant, so the situation needs to be treated as a disaster anticipation process – part of the normal risk management concerns of any enterprise. On a more positive note the situation can be seen as an opportunity for throwing out old and dysfunctional systems (Cromhout 1998)

Obstacles – establishing a compliance process

The US Small Business Administration has published a Y2K checklist for small businesses based on the one developed by the Federal Reserve Board. Links to additional checklists, definitions, and resources are provided as well. Many consulting firms have developed different strategies for a variety of systems, but in essence they contain the same basic structure. Particular mention must be made of the checklist published by Deloitte and Touche identifying the activities involved in achieving Y2K compliance (Deloitte and Touche 1998d). It is not the intention of this article to detail the activities involved as these will vary according to the business situation concerned. However, it is clear that the major activity in the whole process remains one of testing.

In July 1997, Steve Gold, reporting for *Newsbytes* wrote as follows:

> 'According to Taskforce 2000, the Year 2000 problem group set up by the British government,

> companies working towards a resolution to their Year 2000 problem must recognize that testing is at least 50 percent of the solution and that, unfortunately, many companies will be unable to test their own systems without disrupting their operations ... At least 50 percent of the problem remains in the testing of these systems to remove the risk of system failure on 1st January 2000. However, for organisations such as banks and financial institutions, who require 24-hour system availability to support ATM and telephone banking networks, there is no ideal time to undertake this testing ...' (Gold 1997).

The US Small Business Administration's guidelines include advice on how to assess system readiness, ways to test and validate the system, and how to check personal computers for Year 2000 readiness using a bootable DOS floppy diskette. In personal computers, the Millennium bug could be located in any one or all of three locations – the BIOS, the operating system or the applications software. Once turned on a PC relies on its BIOS (Basic Input Output System) to check the data stored in its Real Time Clock (RTC). The operating system takes the date and time from the RTC and applications draw date/time information from the operating system.

Year 2000 compliance for applications software should be determined through the manufacturer. However, a diagnostic software utility may be downloaded free of charge from the Web site of the US National Software Testing Laboratories (http://www.nstl.com/html/ymark-2000.html). The program, called YMARK2000, temporarily sets the computer's internal clock to read ten seconds before the millennium and then monitors its ability to roll over to 2000.

Possibly to align themselves with the occasion of the 500 days before Y2K, Novell announced on 19th August 1998 that:

> 'Novell <http://www.novell.com/> has changed its upgrade policy for making a version of its software Year 2000 compliant. Novell has decided against charging users of its NetWare 4.10 operating system for a full upgrade to NetWare version 4.11, which makes the operating system Year 2000-ready. Instead, the company will post a free Year 2000 update patch for NetWare 4.10 on its Web site in the fourth quarter, escaping the possibility of lawsuits filed against the company by disgruntled customers who claim there is not enough time to do a full upgrade before the year 2000 arrives. Prior to the decision, customers had been told they would need to pay for an upgrade to version 4.11 to ensure their software would continue to work after the century date change. The upgrade also included new features' (Leuning 1998).

Users of IBM-compatible PCs might face problems if their systems run on an early Pentium processor or an older chip. More recent Pentiums or Pentium II processors should be compliant, but some Pentiums, 486s and other processors are not.

Microsoft Windows also exhibits mixed compliance. Windows 3.x and older revisions of Windows 95, may need to be upgraded, but Windows 98 and Windows NT 4.0 have no century date problems. Microsoft maintains a Web site with information on the millennium compliance of all its products including Word and Excel (http://www.microsoft.com/year 2000/).

Apple Macintoshes and compatibles have been compliant since they first came on the market in 1984, but Apple still maintains a Web site where millennium information may be found at http://www.apple.com/macos/info/2000.html# macos. Similarly, Sun Microsystems maintains a site for checking compliance with their Unix operating systems platforms at http://www.sun.com/y2000. All should be subject to thorough testing.

For larger, mainframe systems, Murray and Murray (1996) give a useful format for developing a compliance process in which

- The problem is defined.
- The solution strategy is set forth.
- The algorithm is described.
- The algorithm is translated into a generalise pseudocode.
- The documented source programming code is exhibited in an assembly post listing.
- A sample of the test results is displayed.
- Comments on the source code are presented.
- A brief tutorial on applications is presented. Each chapter's source program code is in the form of a subroutine coded in line with a calling test program.

  > 'The languages used is IBM's ALC (BAL). Thus, the subroutines can be used in other ALC programs or can be called by COBOL or PL/1 under MVS, called by RPG or by COBOL, used under VSE either in batch environments, or used under CICS/VS in command-level programs. Example IBM VSE linkage conventions appear in the appendices. All source code was assembled and tested under VSE or MVS. For ease of use the assembly post listings are presented in the book' (Murray & Murray 1996:xvi–xvii).

A different approach is taken by Delohery and Buckso who recommend a combination of configuration management/ version control, the right tools, and system reengineering. Again the purpose of this document is not to reiterate those recommendations as the original is readily available. However, what is important is that their emphasis is again placed on testing and using the right tools to do so.

> 'The positive result of the project is an analysis of the complexity of each source. Those sources with high complexity become candidates for selective rewrite. That rewrite of a program using structured methodologies will reduce overall maintenance costs and simplify future enhancements. All applications will then continue into the 21st century. In addition a strong quality-management program, with a dependable development and testing environment for the

future, will have been built for a relatively small incremental investment. The quality-management processes put into place will allow the organisation to develop and deploy new products and services that will significantly increase both operational effectiveness and competitiveness' (Delohery & Buckso 1997).

As readily accessible and giving as much emphasis to the role of testing, are the pamphlets prepared by Deloitte and Touche. They make the point that testing could take as much as 50% of the Y2K project time and resources, and it is therefore advisable to choose the most appropriate testing strategy with care.

'Given the total effort required for testing, and the necessity to repeat tests over the course of the project, it is also sensible to consider approaches which use tools and automation as much as possible ... A variety of tools are available to aid with these tasks and should be included in the test strategy where possible:

– Test data generators – used to large volumes of test data based on input parameters.

– Comparison utilities – used to compare original screens, reports and files to their Year 2000 compliant versions.

– On-line capture and playback tools – used to create consistent, reusable input.

– Test coverage analysers – used to highlight the percentage of the program that has been executed.

– Virtual data utilities – used to simulate the date as being in the year 2000 for testing purposes.

– Data migration and data update tools – used to manipulate data so that it reflects future dates.

– Environment simulators – used to create a test environment on a workstation before the programs are moved to the native mainframe environment.

– Execution simulators – used to step through a program without executing it so that the programmer can follow the control flow.

– Debuggers – used to set break points in the program code so that the execution of the program will be interrupted at these points' (Deloitte and Touche 1998e).

However, to distinguish between the capabilities of the Year 2000 tools on the market requires an understanding of the technical workings underpinning the tools. Deloitte and Touche offer tool selection criteria to ensure that costs, the number of tedious laborious tasks and the likelihood of errors are reduced, while coverage and long-term value are increased (Deloitte and Touche 1998f).

Obtacles – legal considerations

The following are general statements responding to common legal inquiries, provided solely for informational purposes, and not as legal advice. Legal conclusions will vary depending on applicable local and national laws; and legal conclusions may vary depending on individual circumstances. Specific legal inquiries should be referred to appropriate legal counsel.

Although the cause of, and the fixes for, the Year 2000 problem are technical (software assessment, re-engineering and testing), minimizing potential liability, assessing legal rights and pursuing valid claims are legal issues. A company's failure to focus on the legal issues relating to the Year 2000 may cost the company more than the company's expenditures for its technical fix. Legal risk control should be a central component of any significant Year 2000 remediation program.

Most of the damages resulting from the Year 2000 will be economic. Many courts have held that economic damage alone is not a sufficient basis for legal action. Such actions are usually handled as breach of contract cases (the software did not perform per the warranty). Further, most non-compliant software was the result of an economic decision to refer to the year in a two-digit format and therefore the product performed as designed. However, manufacturers of software, hardware or equipment that control aircraft safety or medical devices and hospitals will have greater exposure if there is a software or product malfunction since such a malfunction could result in bodily injury.

Throughout the world there is increasing focus on the possibility of litigation to assist in determining who is responsible for the Year 2000 problem and who is responsible for the cost of fixing it. This focus usually centers on several considerations (Deloitte and Touche 1998j).

Copyright

Possession of source code does not create the right to copy or modify the source code. Many escrow agreements provide for the release of source code, without granting a license to use it, and even if written permission has been obtained from the licensor, it may not apply to an independent third-party contractor making the modifications. While the client has the right to hire someone other than the original developer to perform Year 2000 modifications, the author of the software holds the copyright and therefore the right to 'prepare derivative works'. Review of the circumstances under which the systems were acquired, including development contracts, transfer documents, assignments and licenses are thus crucial (Deloitte and Touche 1998k).

Contractual liability

The scope of the warranties which accompany a software transaction can be determined from the transaction documents, sales materials or product manuals which accompanied the sale. These warranties may be express warranties – a statement presented as fact, a product description or a promise concerning the product – or implied warranties – warranties of merchantability and of fitness for the purpose for which it was produced. If a software product could be expected to have a ten-year life span or to calculate

dates beyond the Year 2000 in ordinary circumstances, failure to provide a Y2K product would constitute a breach of warranty.

Delictual liability

This liability relates to wrongful acts on behalf of the vendor of the product. They include fraud, misrepresentation, negligent misrepresentation, professional malpractice and negligent design and strict liability. Specific legal questions regarding an enterprise's precise liability should be discussed with a qualified attorney (Deloitte and Touche 1998j).

Many enterprises at this stage are seeking to limit their potential liability given the uncertainty of the situation. Most claims for non-performance will be based on or governed by the original license agreement. Most non-compliant products were purchased several years ago. In some cases, the time to bring suit may be expired; and in other cases, time is running out. Further, many license agreements contain express disclaimers of warranties and/or clauses limiting liability. Courts typically uphold such provisions. Even if a warranty does apply, the customer may be contractually obligated to bring a suit for breach of contract within one year after the date of discovery of a breach. IBM, in a recent letter to its customers, has already indicated that many IBM products are not Year 2000 compliant, and that it will not 'fix' its non-compliant products (Hassett 1997).

However, it is helpful to identify situations where liability can be limited for both vendors and buyers. To do this it is advisable for them to seek legal expertise, as stated above. Vendors can limit their potential contractual liability by disclaiming warranties. Such clauses would state clearly that the terms of the contract are operative and that representations not contained in the contract are inoperative. A liquidated damages provision can be included and recovery can be limited to the repair or replacement of the software as long as they are negotiated between the parties and made explicit in the contract. While there are tremendous opportunities for vendors seeking to assist firms achieve Y2K compliance, the situation is fraught with legal pitfalls. Some of those are identified in another of the specialized pamphlets produced by Deloittes (Deloitte and Touche 1998m).

Similarly for software purchasers there are ways to protect their rights by limiting their liabilities and ensuring that damages resulting from defective software can be recovered. Most vendors will be prepared to modify their standard printed contract, and purchasers are entitled to the assurance that they get what they pay for. Objectively determined performance criteria should be stated in the contract. Again, consulting a qualified legal counsel is essential to limit the potential liabilities or damages (Deloitte and Touche 1998l).

Besides the sales or purchasing contracts, it must be borne in mind that service level agreements usually provide for downtime. Failure of software or hardware at the turn of the millennium may well be considered in that context. In many cases, the original vendors of hardware and software will face no legal responsibility for the Year 2000 problem. Actual liability could depend on a variety of factors, including the terms of the original license agreement, applicable laws, and the whims of the courts.

For those contemplating legal action, it must also be borne in mind that customers have responsibilities. They must be certain that the product they purchased met their needs and that it was properly maintained and serviced. If they suspected that the product might fail, they would need to establish that they had done everything possible to avoid a failure. However, vendors are generally declining to repair or replace non-compliant systems (other than full replacement at full price). In most cases, the vendors have a sound legal basis for taking this position.

Opportunities

Any Year 2000 project affords an organisation the opportunity to implement the quality management programme that has been on the drawing board for ages. It can be the vehicle for radically transforming the way things are done into the way things should be done. Or it could be considered to be part of the normal risk management procedures of a company intelligently anticipating a potential disaster.

Another positive result of a Year 2000 project is an analysis of the complexity of each source. Sources with high complexity become candidates for selective rewrite. Industry statistics confirm that the defect rate of a program increases in direct proportion to the complexity of the code. A rewrite of a program using structured methodologies will reduce overall maintenance costs and simplify future enhancements. Depending on time constraints and resource limitations, the actual rewrite may be deferred. Deloitte and Touche offer advice on how to undertake an analysis of applications to decide strategy for meeting the Year 2000 compliance requirement (Deloitte and Touche 1998a).

For some organisations, replacement of information systems is seen as the best option. Tony Cunnington, chief executive officer of South African financial software development house Hill Cunnington & Associates (HCA), is reported as saying that replacing software with a modern package to bring computer systems up to date is a good alternative to trawling through millions of lines of code.

> 'Many upgrades currently being undertaken by local companies are geared only at preventing the system from crashing when the millennium arrives. This means companies are investing a great deal to stay exactly where they are today. Replacement is certainly the most viable option for companies that utilise standard off-the-shelf software, including financial systems. Many software programs have a built-in, flawless, bug-free transfer of data without the risk of duplications or omissions' (*Replacement is best option* 1998).

The timing of the decision can also be turned to the advantage of the enterprise. It may be seen as best to wait until just before the millennial change to install any new

system so exploiting the advantage of the learning process through which the international software industry is proceeding.

Seeing Year 2000 compliance as an opportunity to revise disaster recovery and business continuity plans puts a positive light on expenditure. Given sufficient publicity and marketing, this can be used to enhance marketability and product offering. Quality improvement by upgrading software or business processes has a market value that should be exploited. Companies can make much of the renewal of their technology base.

Carruthers (1997) reports that some benefits directly caused by the Y2K team have included improved configuration management, improved RFP practices, centralised contract management, centralised vendor management, improved testing processes, environment, and facilities, and improved software maintenance tools and processes.

There can be no doubt that Y2K is an opportunity in many ways – to do a better job, smarter; to gain publicity for improving systems and services; or to exploit the situation creatively, in the same way that businesses and industry have always exploited natural and human disasters.

Opportunities after 1/1/2000 – picking up the pieces

At this stage no one can anticipate what will happen as the millennium rolls over, although it is suspected that, instead of celebrating, many people will be soberly listening to the news from eastern countries, especially technologically advanced countries, to discover what facilities and amenities collapse. This will give them a short opportunity to anticipate and perhaps avert any possible disasters. However, 1st January, 2000 will be a Saturday and many businesses will be closed. The impact may therefore only be felt on Monday 3 January when people return to work and normal activities recommence.

It is to be expected that even those institutions that have initiated compliance programmes may not have completed them on time. Others, believing that they are compliant, will discover programmes, applications or equipment that has been overlooked and will need to remedy the situation.

What is clear is that two groups of people will be in heavy demand. Feverish activity will commence as information systems technologists are inundated with requests for help in picking up the pieces, scanning non-compliant software, installing compliant components or packages, and reinstating applications which have collapsed overnight.

In addition to the technical consequences, there will be immense legal implications as businesses or individuals seek to apportion blame and to obtain financial compensation from likely sources. Auditing firms with insurance cover against such eventualities are likely to be the primary targets for such litigation, as are government and quasi-government bodies that might be considered soft but lucrative targets for such litigation. Particularly vulnerable are those northern hemisphere countries with a technologically sophisticated infrastructure, caught in the grip of winter, facing the possibility of power cuts, the collapse of telecommunications and transportation facilities, and other events which could have implications for loss of life or damage to health.

In any event, there are considerable opportunities for profitable enterprise. Information systems technologists and managers, software developers and systems vendors all stand to benefit from providing remedial services without the risk of stipulating in advance that their work will be Year 2000 compliant. For the innovative entrepreneurs, advantages are to be gained from flexibility, customisability and the provision of a wide spectrum of solution sets. For the institutions having to consider such options, any earlier attempts to ensure Year 2000 compliance will stand them in good stead and minimise costs and damages. Planning activities to deal with any eventuality that may arise both before and after 1st January 2000, can only be of benefit. However, there is little evidence to suggest that much thought is being given to the problem of picking up the pieces in January 2000.

Conclusions

There can be no doubt that no matter what is done to prepare for the millennium roll-over on 1st January, 2000, the consequences are unpredictable. Mainly negative connotations emerge from the publicity being given to the matter. This deliberately creates a sense of urgency to ensure that as many people as possible become aware of the implications and start to do something about them. However, the fact that no one can anticipate exactly what might happen and from where the threats will come creates a sense of helplessness. It is compounded by the fact that the problem is not simply technical and able to be rectified by rewriting programming code, or installing Year 200 compliant systems. Threats may result from legal, social, political or economic consequences of the millennium roll-over.

It can be accepted that some organisations will be compliant, while many will not. Those that are not may well have a major impact on those that are. For many people this could leave a feeling of helplessness and purposelessness since a solution may be well out of their reach. Whatever they do, however much resources or effort they plough into achieving Y2K compliance, success may elude them as a result of failures in other enterprises beyond their influence. Although this may appear to be a negative view, there are indeed many positive sides to the situation.

Certainly, the process of achieving, or attempting to achieve, Year 2000 compliance has many advantages for those undertaking it. Success has benefits such as a better understanding of systems and their hardware components, as well as creating numerous opportunities for business advancement.

Publicity being given to the whole situation has created opportunities for businesses to analyse their hardware and software according to proven methodologies. This article has shown the standards that are applicable to conformity in South Africa and how they relate to those applicable elsewhere. Recognising that compliance alone is insufficient to

ensure peace of mind for the conscientious manager the significant risks associated with the whole situation are identified and discussed. Suggestions are made as to who is responsible for addressing those risks, and how to minimise them, bearing in mind that many of them relate to legal issues and require specialist legal counsel.

To keep providing a positive emphasis, any suggestions about a 'silver bullet' which will be a panacea to solve the wide spectrum of problems are dismissed and positive suggestions about what can be done to calm the concerns of the stakeholders are made. Understanding what those concerns are enables managers to identify ways that the compliance process can be approached to enhance a company's business offering and competitiveness rather than just being seen as a non-productive expenditure of resources to avoid a potential problem of unknown proportions.

Business opportunities arising from the Year 2000 problem are many and varied. They depend on the perspective of the individual entrepreneur and the resources that can be applied to achieve them. After all, business and industry have always exploited natural and human disasters, and the Year 2000 is equally amenable to positive exploitation. One of those entrepreneurial opportunities lies in providing facilities to help businesses pick up the pieces after 1 January 2000. Or the information systems specialist that remains the most positive aspect of the millennium bug and one that is little dealt with in the published literature. It is the one area that deserves intensive research to the positive benefit of all concerned.

Acknowledgements

This article, in a fuller form and with a different focus, was originally presented in partial fulfilment of the requirements for the Bachelor of Commerce Honours degree at the University of Cape Town. As in the original, warm appreciation must be recorded for the contribution made by Ms Cindy Cromhout of Deloitte and Touche in providing the author with the opportunity of discussing the matter with someone dealing with the problems of Year 2000 compliance on a daily basis.

References

British Standards Institution. 1997. *DISC PD2000-1 A definition of year 2000 conformity requirements.* London: BSI.

Capers Jones. 1998. *The global economic impact of the year 2000 software problem.*(Version 5.2) Burlington, MA: Software Productivity Research.

Carruthers, H. 1997. *Unexpected year 2000 benefits.* [Online]. Available: http://ourworld.compuserve.com/homepages/goal2000/y2kbeni.htm

Cromhout, C. 1998. Personal interview. 29th May.

De Jager, P. 1993. Doomsday 2000 *ComputerWorld*, Sept 6. [Online]. Available: pdejager@year2ooo.com

De Jager, P. 1996. *Biting the silver bullet.* [Online]. Available: pdejager@year2000.com

Deloitte and Touche. 1998a. *Selecting a Y2K strategy.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998b. *Impact assessment.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998c. *Risk assessment.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche . 1998d. *Y2K Activity list.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998e. *Y2K testing strategy.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998f. *Selecting Y2K tools.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998g. *Implications for directors.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998h. *Implications for auditors.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998i. *Impact on the JSE.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998j. *Legal issues and liabilities.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998k. *Beware of copyright.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998l. *Limiting potential liability.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998m. *Vendor liability.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998n. *PABX, microprocessor, etc.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998o. *Process control systems.* [Online]. Available: http://www.dtcas.co.za

Deloitte and Touche. 1998p. *Personal computers.* [Online]. Available: http://www.dtcas.co.za

Delohery, P.D. & Buckso, J. 1997. A blessing in disguise: year 2000 projects can be an ideal excuse for business process re-engineering. *Datamation*, 43(10):29(2).

Gerner, Michael. 1996. Why has the year 2000 problem happened? [Online]. Available: http://ourworld.compuserve.com/homepages/goal2000/reasons.htm

Gillin, Paul. 1997. Y2K pledge. *Computerworld*, 31(38):2(1).

Goal2000. 1996. Some additional background on Y2K math. [Online]. Available: http://ourworld.compuserve.com/homepages/goal2000/y2kmath.htm

Gold, S. 1997. Testing is key to year 2000 resolution - British Govt. *Newsbytes*, July, 29th. [Online]. Available: http://www.newsbytes.com

Gordon, G. 1998. Race against the clock to defuse software time-bomb. *Business Times*, 29 March. [Online]. Available: www.y2k.org.za

Hassett, D.B. 1997. *Frequently asked questions about the year 2000 problem.* [Online]. Available: dhassett@wmcd.com

Luening, E. 1998. *Novell makes Y2K upgrades free.* [Online]. Available: erichl@cnet.com

McCright, J.S. 1997. Simulating Y2K risks. *PC Week*, 14(41):22(1).

Millennium trading curb threatened. 1998. *Business day,* 18 March. [Online]. Available: www.yak.org.za

Murray, J.T. & Murray, M.J. 1996. *The year 2000 computing crisis: a millennium date conversion plan.* New York; McGraw Hill.

North, G.1998. [Online]. Available: http://www.garynorth.com/

Replacement is best option. 1998. *Business times*, 28 March. [Online]. Available: www.y2k.org.za

Scheier, R.L. 1997. Economist predicts Y2K-based recession. *Computerworld* , 31(38):12(1).

Wilson, T. 1997. Year 2K: ready or not? *InternetWeek,* 684:79(1).