Speech

Y2K Audit and Certification *

A. Vasudevan

The Year 2000 problem which appeared to be an exceedingly difficult one only a few months ago now seems to be within the grasp of resolution. In the Banking sector, the Year 2000 compliance has been complete. This was rendered possible because the efforts at initiating the whole process of Year 2000 identification and testing began quite early. Besides, the sector has had the advantage of obtaining support from the top managements and Boards of banks.

The latest indicatiions in regard to the Year 2000 compliance in other sectors give considerable satisfaction. Almost all the non-banking sectors are confident of gaining compliance soon, by end September or October at the most. Information on this matter is being regularly monitored and disseminated by the National Y2K Action Force. The developments are regularly put on websites and reported in newspapers. Some institutions have on their own begun to advertise about their compliance. The concern about the possible failures in interconnected sectors has waned and public confidence in our successful approach has improved sharply.

From the point of view of international institutions and investors, this is very good news. But it is not mere compliance on which we should focus our attention. The real issue from the nation's perspective is now on business continuity. The Year 2000 contingency planning is what matters most now than ever before. And, contingency plans by definition would have to be operable in need and contingencies. Since they have to ensure continuity of business operations, they would have to be such as to be in a position to handle a good chunk of volumes of business and help the businesses to run in an efficient manner during the transition to the Twenty-First century. Surely, they would not entail provision of mere backup for computer systems. For, if computer systems fail, their backup systems which are replicas of the original, will also fail. Contingency planning has to be therefore, about focussing on core activities in a market and business context, so that the businesses survive.

It is necessary to test contingency plans as frequently as possible and put them into operation well before the date of change to the new Millennium, even where there is full confidence of 100 per cent success in the resolution of Year 2000 problem. This is important because human endeavours in general need to be constantly reassured of their effectiveness.

The enormous resources so far spent on areas where computer systems are intensely used and are interconnected and where operations may have embedded chips have been worth the money since financial and non-financial businesses which have recently adopted modern technology and computerised operations have done so, not only for improving efficiency in their day-to-day operations but also for minimising risks associated with the businesses. The literature on Year 2000 and contingency planning have shown that at least two major risks need to be clearly addressed. One is the operational risk arising out of the failure of internal systems and problems with infrastructural facilities such as elevators, air-conditioning / heating, backup arrangement and disruption in the services of utilities such as water, electricity, telecommunications, etc. Some of these could be external to institutions concerned but strategies will have to be put in place to control the risks arising out of exogenous factors. The second is the credit risk which

occurs when financial loss takes place due to counter-party default or depreciation in the value of assets of the institution concerned. Besides, there could be liquidity risk when financial institutions face unexpected cash flow shortfalls, like for example, due to the inability of business concerns to trade and settle in the context of the Year 2000. Finally there could arise reputational risk when a financial institution is not perceived to have prepared well to address the Year 2000 problem by customers, counter parties, or market participants. This problem can be best addressed by strong disclosures and information dissemination. Public needs to be made aware not only of the status of the Y2K preparedness of each of the sectors concerned. This can be achieved by issuing special bulletins and press releases and publishing balance sheets prominently. Self-assessments could also be placed on Websites, if need be. Those institutions which have sufficiently critical or growing international exposure may need to seriously consider having credible disclosures on websites and in the press.

The Reserve Bank has a crucial role in ensuring that the financial system is not faced with credit and liquidity risks not merely because of its supervisory function but because of its commitment to financial stability. The Reserve Bank has specifically placed emphasis on the need to set in place in the last quarter of 1999, manually operable systems especially for the accounting and computational systems and test them for their quick and efficacious operation. This is possible since a large number of banks in India are not fully computerised and interconnectivity exists only in specific areas.

Let me now come to terra firma and issues pertinent to this conference. It is important for banks and other institutions to have greater comfort and confidence in their business continuity through appropriate auditing, preferably a third party one. The certification of computers, hardware, software systems including application software by auditors would bring about a reassurance that institutions and the public at large seek about the real time movement of transactions into the new Millennium from the present century.

One of the important decisions to be made by institutions pertains to the choice of the audit agency. There are some who consider that there are not many qualified third party Y2K auditors. There are some who favour audit to be performed by technically competent in-house experts. There are also arguments strongly favouring external (and preferably) third party audit agencies.

It is difficult to contest the validity of each of these arguments. Although on the face of it, third party audit appears to be rational, the competency of the firm / organisation chosen for audit and the tools adopted for auditing is of paramount importance in ensuring that the certification issued by the agency satisfies not only internal requirements but also international standards. While agencies often provide information about their commitment and past record, they need to also specify the personnel to be attached for the tasks assigned, their experience and competence. This is essential because a perception has emerged to the effect that the assigned personnel for audit purposes are not qualitatively much different from the internal auditing teams. Such perceptions gain credibility when one finds the high costs borne for audit/certification, and the limited clear benefits visible from such auditing. Given the high costs and the uncertainty about the available pool of skilled third party auditors /certifiers, a determination would be made as to whether the issue of third party auditing should be mandated in some cases where internal expertise is strong.

Let me now deal with the coverage of audit. An important consideration is the hardware/software to be subject to audit. In the case of the hardware, operating systems and Systems software (middle-ware and networking products), specific and clear guidelines are available on the fixes, patches or compliant versions. Their acquisition and performance in relation to the dates of the millennium have to be seen. In the case of software, not all programs in use are date sensitive. Similarly, there could be some portions of computer equipment such as Hubs in a

LAN environment which may not be date-critical. A critical component is the Real Time Clock - the RTC and its relevance to the application software which is perhaps the most crucial item to be checked for Year 2000 compliance, because, without this, the entire computer system may not even start functioning at the dawn of the millennium. A decision on whether such components have to be subjected to the audit process or not has to be taken internally. The soundness of such a decision is often in question, but the role of an auditor in concurring with such exclusions becomes vital.

Let me now discuss the auditor's point of view. The role of a Y2K auditor is to ensure that neither the performance nor the functionalities of the hardware / software is affected prior to, during and after the advent of the Year 2000. This implies that the auditor may have to know the complete functional details of the hardware or software or the back data as the case may be. In order to facilitate the auditor's task, it becomes essential that the software is furnished alongwith full details such as program flow / logic in respect of the usage of date, the seed list of date related functions in the software programme, the various programs, subroutines, etc., having an impact on the entire application software package. It is well known that while this is an essential prerequisite for all auditors not only from performing the audit but also to gauge the requirement of personnel to perform the audit and in assessing the cost implications for the audit process itself, the provision of these details becomes a difficult proposition in case the application software has been developed in house or if the documentation is not fully available.

Most of the hardware and software in use are not individual islands of operation but are pieces that function in close coordination with other components. Most of these components - both in the case of hardware and software - are not developed by the same vendor (or in-house as the case may be) but are standard third party products. These products have been certified by the respective suppliers/ producers and it now becomes the responsibility of the auditors to appraise the impact of the third party products in regard to the entire date sensitive hardware/software. It is generally true that auditors are capable of performing this function to the satisfaction of their clients.

One of the issues that have no direct consequence to the Y2K problem as such but has nonetheless a definitive bearing on it relates to the legal implications of certifying Y2K compliance. While utmost care would be ensured in checking the total compatibility to the Year 2000 problem; the legal implication of any probable losses suffered directly or due to consequential losses on account of any failure related to Y2K, is an aspect that deserves attention. It is not very clear whether the certification / audit provided for would also attract any direct or consequential impact in case of failure. While such a situation may not arise in our

country, there is the imperative need for audit to be carried out in a scientific, objective and exhaustive manner taking all possible facets into account so as to ensure that there is not even a remote possibility of the audit certificate proving itself to be negative with the onset of the millennium.

One of the buzz words in the financial world these days is 'transparency'. But it is most relevant in the present context of Year 2000. Complete transparency is required in the practices and measures taken to resolve the Year 2000 problem. It is essential that the audit and certification of Y2K is also as transparent as possible. This would imply that relatively clear and categorical statements of certifications are required for providing enhanced public confidence.

There are about 100 days from now on for the industry and the user community to complete the entire process of Y2K audit and certification. It is possible that the available auditor support may not be adequate to cover the well spread offices throughout the country of all the banks, financial institutions and major corporates. Y2K auditors would have to rise up to the occasion and in close co-ordination with the users ensure that the measures taken for ensuring Year 2000 compliance would see the country safely through the dawn of the new millennium.

*** Keynote Address by Dr. A. Vasudevan, Executive Director, Reserve Bank of India at the National Seminar on Y2K Audit and Certification at Hyderabad, hosted by the Department of Electronics and CMC Ltd. on September 10, 1999.**