

2. BROAD APPROACH TO THE PROBLEM

2.1 The wide range of Year 2000-related risks necessitates that the managements implement a targeted, multifaceted action plan to smoothly move over to the millennium. Addressing the Year 2000 issue consists of undernoted seven elements:

- Developing a strategic approach;
- Creating organisational awareness;
- Assessing actions and developing detailed plans;
- Renovating systems and equipment;
- Validating the renovation through testing;
- Implementing tested, compliant systems; and
- Contingency planning.

The Reserve Bank of India has adopted the definition of British Standards Institution for Year 2000 conformity. Accordingly, 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 an interruption in operation

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

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

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

Definition of ‘Critical’ Systems

The distinction is made between ‘Critical’ and ‘non-critical’ systems in respect of Year 2000 compliance. This is done to ensure that attention is focussed on those systems, which are likely to have the most disruptive impact should they not be Y2K compliant. The Reserve Bank of India has defined a system to be critical if its failure would:

- result in a substantial loss (either in money or goodwill of the organisation);
- have a significant impact on the operations of the institution; or
- adversely affect its customers/counterparties for an extended period of time (e.g. over 24 hours, but this could vary depending on the type of business).

This definition covers payments, accounting, treasury, risk management, front office, communications and operating systems directly supporting essential banking services.

2.2. Origin and Scope of the Problem

Since the earliest days of computer programming, in order to economise on computer memory two digits were used to represent the year in date fields (YYMMDD). Even as recently as the 1980s, few believed that the applications being developed by them would still be running in the year 2000. The Year 2000 problem exists because, at the turn of the century, a two-digit representation of the year will be interpreted in many applications to mean 1900, not 2000. Thus, at the century date change (or even before), a large number of computer systems, software programs and embedded chip devices currently in use will produce errors or malfunction -- unless the date or program logic is modified. Many calculations will either indicate that financial or accounting transactions have been open for nearly one hundred years or produce negative numbers. New files may not be recognised as the most recent data, causing current files to be erased or archived as old data.

The problem has the potential to affect both computers and the embedded processors built into all kinds of modern equipment. Mainframes are particularly vulnerable as individual components may be of widely different vintages and a single non-compliant component could affect the entire system due to linkages amongst different system components. Mini-computers and personal computers may also be affected. Additionally, telecommunications equipment often has built-in date features that must be identified, tested and corrected where necessary. When the readiness of pre-renovated systems is assessed, it is often the case that more systems than expected malfunction under simulated Year 2000 conditions. Due to the interconnectivity of systems, even applications that were originally designed to comply with the Year 2000 have been found to require certain modifications. With regard to embedded processors, any operation that functions using date-sensitive technology may be affected. Many applications whose functions do not appear to rely on dates may have processes that are date-sensitive. Embedded chips that are date-sensitive and non-Year 2000 compliant are installed in millions of systems worldwide. These chips are integral to a wide range of devices and systems, including Automatic Teller Machines (ATMs), medical pacemakers, heating systems, plumbing, electricity, transportation including rail engines and aircrafts, Airports, Air Traffic Control units and financial data transmission systems. Unexpected, undesirable results could occur in many contexts, e.g. bank vaults, lifts, etc. Identifying and renovating (or replacing) the chips that may cause disruptions may be an extensive, complicated and challenging endeavour for many organisations.

For financial market participants, the Year 2000 problem is critical. Financial Institutions rely heavily on automation to manage information. If automated applications fail to work properly, it will be difficult if not impossible to conduct business. While an isolated non-Year 2000 compliant line of code should be relatively easy to repair, the number and complexity of date-dependent computer programs and embedded chips/controllers in use means that the remediation effort (fixing the programs) is very often a highly resource intensive process. Moreover, given the financial sector's

reliance on various infrastructure providers (water, power, telecommunications, payment systems, securities exchanges, etc.), the readiness of these systems has enormous implications for the continued functioning of the financial system. Operators of these systems are faced with significant Year 2000 challenges; unfortunately, the readiness of many of these complex systems is less than certain. Mere assertions that computer applications are unaffected cannot be seen as adequate substitute for rigorous assessment, remediation and testing efforts that should be undertaken by financial market participants.

2.3. Impact on Financial Markets

The date-dependent calculations performed in a variety of financial transactions (e.g. ageing of information, calculating interest rates, etc.) expose a financial organisation to serious business disruption should they fail to be ready for the millennium change. For, applications vulnerable to Year 2000 problem affect all areas of the business: the front office, the middle and back offices, the customer delivery system, and management information and decision support systems. The task is particularly daunting for financial firms because it is not just internal to the organisation. Many organisations maintain automated linkages and interdependencies with correspondents and customers, both domestically and internationally. For larger institutions that provide a wide range of products in many countries around the world, many of these applications are interdependent and some are interactive in real-time processing environments. If applications are not able to work together properly, significant problems could develop. The interconnectedness of financial organisations is especially clear in the context of their reliance on the financial market infrastructure. Payment systems, settlement agents, clearing organisations, securities depositories, trading systems, exchanges and the various direct and indirect participants in these systems, as well as network providers, are intricately connected. An operational breakdown resulting from insufficient Year 2000 preparations by any one of them may have an impact on participants across systems. For example, a Year 2000-induced operational breakdown that results in delayed funds payments may cause significant liquidity pressures for market participants. To the extent that transactions with counterparties both within and outside that particular settlement arrangement are affected by these delays, there may be knock-on effects, which in extreme cases could have wide systemic implications.

Framework for Achieving Year 2000 Compliance

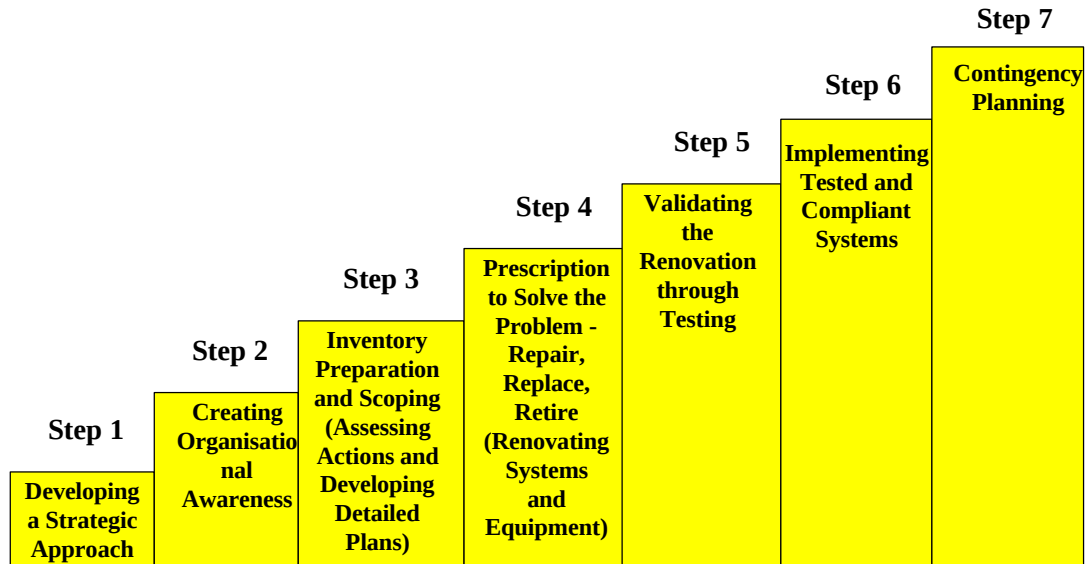


Figure - 2.1

2.4 A Framework for Achieving Year 2000 Compliance

Achieving Year 2000 compliance is simple in concept, yet for large organisations it is an enormous task. The primary goal is to minimise risk to the business. As with all large projects, the development of and adherence to a realistic timetable are major factors in achieving a successful outcome. The Basle Committee on Banking Supervision have provided guidance for banks. Banks in India have been encouraged to follow these international standards and the Reserve Bank of India will monitor adherence to them closely. Though targeted specifically for banks, other organisations may be able to use the following project outline as a starting point. Figure 2.1 gives pictorial form of the steps involved in the Framework for Achieving Year 2000 Compliance.

A Strategic Approach: Addressing the Year 2000 problem must be viewed as a strategic objective and must entail commitment from the highest levels within the institution. The RBI expects the Board of a bank to be involved in this process. The Year 2000 project core group that banks/entities set up have to develop an overall strategy that encompasses in-house systems, third-party service providers, suppliers, customers, counterparties and auditors. A timetable would have to draft and estimate funding built into future budgets. The

same principle has to be applied to various Central Office Departments and the Regional Offices of the Reserve Bank.

Awareness and Commitment: All staff members must be made aware of the implications of the Year 2000 problem and accept responsibility for addressing the problem in their areas of operations. Failure to establish awareness and commitment can lead to omissions, and inappropriate responses or, it could impact adversely on Year 2000 preparations being undertaken elsewhere in the organisation.

Inventory Preparation: An inventory must be taken of all hardware, software, embedded microchips (in cheque-proofing machines, security systems, elevators, etc) and customer and supplier interdependencies. The risk each one of them poses to the business need to be assessed and priorities accorded. In determining the systems that are critical to the operations, the banks and financial institutions should focus on what business functions they perform, and identify the various systems needed to support them. Strategies should be carefully considered, including the role of external parties, the methodologies for renovating programs and the need for additional resources. At the end of the assessment stage, a bank should have detailed plans for the entire project. The assessment stage should be revisited periodically, and certainly whenever an organisation's objectives, processes or external environment change.

Scoping: A critical step for addressing the Year 2000 problem is the assessment of all areas and activities affected by the millennium change and the development of corresponding detailed plans to address conversion of the affected systems. During the assessment phase, it is necessary to determine the size and complexity of the problem and magnitude of the effort necessary to address the Year 2000 issue. An adequate assessment includes consideration of relationships with third parties, including vendors whose products and services the institution uses, other financial institutions, clearing-houses and customers with whom it exchanges data electronically, and customers whose standing may be diminished by significant disruptions associated with the millennium change. The assessment must also go beyond information systems and include environmental systems that are dependent on embedded microchips (for example, security systems, vaults, telephones, faxes, heating/cooling systems and elevators). This prioritisation will occur after a risk analysis of

the various systems has been conducted. The action plan will differ according to the size and complexity of the financial institution. The institution must identify the required resources (personnel, budget and external resources) needed to implement the action plan. The action plan should outline which systems will be replaced, upgraded or otherwise modified and what the conversion process will entail. The action plan should also include a concrete timetable for meeting each element of conversion. This timetable will establish target dates against which to measure slippage in the implementation of the action plan. This timetable should include ample time for testing.

Prescription to Solve the Problem – Repair, Replace, Retire: This process involves modifying, upgrading, replacing, outsourcing or retiring the hardware and other peripherals, operating systems, applications that are not Year 2000 compliant. International regulators have generally chosen end 1998 as the date for completion of the renovation process. Banks in India are well into the renovation stage and indications are that renovation of critical systems will be substantially completed by end 1998.

Testing: Year 2000 testing for banks is of paramount importance because the tests must be conducted on all critical applications, yet the banking business must continue as usual. Industry analysts expect the testing phase to consume more than 50% of the time and resources devoted to the Y2K compliance process. The testing process should cover the hardware including equipment/embedded systems, operating systems, key software utilities - backup, software development tools, applications software, data bases, movement of data between systems, all interface software with the other banks and financial entities, customers, etc.

In order to make objective assessment of the compliance, test records form a critical data. It is important for the banks to look at the test records to conclude that adequate testing has been conducted. Record keeping for test results might become a crucial data in case of potential litigation issues. Test results should be analysed and compared against expected results. Any deviations in the test results should be assessed against the testing objectives laid down for that software component. This analysis should enable the acceptability or otherwise of the software component along with the identification of the residual useful life of the target system.

Implementation: Once systems have been thoroughly tested in a separate test environment, they can be returned to production. This involves careful co-ordination to ensure that changes in one system do not affect the operation of other systems.

Contingency Planning: Financial institutions must develop contingency plans for the Year 2000 problem to prepare for possible computer disruptions. Renovation of systems and carefully planned testing inhouse or by vendor, in addition to the testing by independent service agency could reduce the possibility of computer disruptions materialising in the year 2000. However, despite every care and effort, computer disruptions could still take place. In making contingency plans, it should be noted that in the event of the Year 2000 computer disruption, back-up computer systems cannot be counted on because the technical structure of the back-up systems is likely to be exactly the same as the acting systems and will fail to operate properly for the same reason.

Computer disruption caused by the year 2000 problem is similar to a system failure of both the main system and its back-up caused by hardware / operating system / application software. The contingency plan for such a system failure is to shift operations from online business procedures to paper-based procedures, and the contingency plan for the Year 2000 system failure would likewise be to shift business operations to paper based procedures. Individual financial institutions and payment and settlement systems may put in place contingency plans for system failures of active and back-up systems, to keep up the operations going on.

When making contingency plans for the Year 2000 problem, it must be noted that system failure due to the Y2K problem differs from other system malfunctions or failures because disruptions would materialise simultaneously in many financial institutions, their counterparties and payment and settlement systems. In the new millennium, some financial institutions and payment and settlement systems that have not conducted sufficient Year 2000 tests to verify their computer systems may face system failures simultaneously. In such an event, online business procedures would have to be migrated to paper-based manual procedures. To adequately prepare for such situations, it is necessary to find out the points where paper based processing would establish appropriate disaster backup arrangements and procedures in case of contingency so that operations of the financial industry are not

disrupted.