Appendices

Appendix A

The Year 2000 Challenge in more detail

Origin and Impact

1. Since the earliest days of electronic computers, programmers have used two digits to represent the year in date fields (YYMMDD). While many newer applications are Year 2000 complaint, many older applications upon which compliant application is Year 2000 compliant without appropriate analysis and testing poses substantial risks.

2. Further complexities to the issued are introduced by others considerations such as the use of reserved values such as using 99 in the some way. Even before 2000 is reached, some applications will start behaving badly as, in this example, records for the year 1999 will be treated as special files and handled other than normally. Finally, all programs will need to be checked to see that leap year is properly handled in 2000.[2]

3. There is no single way of fixing existing applications or databases. Two of the most common approaches are to add two digits to the year field (CCYYMMDD) or a technique called windowing, which analyses the two digit year field and automatically recognises year under a specified number (say 60) as being 20yy while yeas over the number are recognised as being 19yy [3]. Other fixes are also appropriate as permanent or temporary measures to address particular applications.

4. Applications 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. Because applications are frequently interdependent on each other all interdependencies must be identified and thoroughly tested every time one element in the chain is modified.

5. Making the appropriate changes is complex. Different situations require different solutions. Adding two digits affects the amount of memory and storage space needed and can affect performance with larger records to process. Windowing requires added calculations whenever a date is encountered and can affect performance. Either approach can affect how one application interacts with another. For example, if a four-digit representation for the year is chosen, linking applications that expect to receive only two digits will require further modifications to assure correct communication. Every time an application is modified to be Year 2000 compliant, it will have to be tested against every other application with which there are linkages. Such testing has to be done not only internally but also with correspondents and customers to assure that interdependencies work properly. Because compliant applications become ready to be implemented on a sequential basis, testing will be an ongoing and repetitive process.

Areas Affected

6. The potential for Year 2000 problems pervades virtually every area of an institution. Applications relying on dates are clearly vulnerable. However, many applications that do not appear to rely on dates use dates in ways that are often not apparent to the user such as in file

naming conventions or where the date is part of a key. Wherever dates are used, they must be identified; checked for being compliant and addressed by appropriate change when necessary.

7. All applications are vulnerable regardless of whether they are developed internally or externally. Applications developed by third parties may be especially vulnerable because reliance must be placed on someone else to make the necessary changes. After changes are made, a bank must test the application to see that it works properly in its unique environment. Testing is essential because vendor applications almost always require current or at least recent releases for operating systems or utilities upon which the application depends. If a bank is not current in its version control, compliant applications may fail.

8. Computer operating systems are vulnerable because dates play a crucial role in file maintenance and performance optimisation routines that are invisible to the user. Access control and security systems are affected and could lock out users both logically from automated applications and physically from buildings or departmental areas.

9. hardware is also affected. Mainframes are particularly vulnerable as individual components may be of widely different vintages and single non-compliant component could affect the entire system. Mini-computers and PCs may also be affected. ATM machines or communications equipment have built in dating features that must be identified, tested, and corrected where necessary.

10. Internal communications networks and public carriers have many date sensitive components. Assuring that all problems are identified and made compliant requires carefully designed tests involving both applications and the network/carrier. Environmental and other systems (heating and cooling systems, elevators, vaults, facsimile machines, etc.) also may have both date sensitive software and hardware with embedded computer chips that may have hidden date sensitive elements.

Risks and costs

11. Significant risks exist in not making all necessary changes and thoroughly testing systems. Operational risks are obvious. Failure to have fully operational automated systems can prevent even simple business functions from being completed because manual or other alternatives may not be feasible if processing volumes are sizeable or information exchanges are extensive.

12. Any operational problems immediately become reputational and legal risks as correspondents and clients react to business problems. If significant banks face problems, the systemic implications could be extensive. Consultants estimate that legal costs along could be in the hundreds of billions of dollars if problems are extensive in the industry. Such estimates clearly suggest the magnitude of the strategic risk faced by a bank and the industry more generally.

13. Because correspondents and customers are also subject to the Year 2000 issue, they too must make the necessary changes to conduct business normally. Testing normal connectivity and message transfers with correspondents and customers is essential but not enough. If they have not also made the necessary adjustments to their own systems, they could pose credit and liquidity risks to the bank. Credit officers need to understand the Year 2000 risks faced by their customers and how well their customers are managing these risks.

Current financial performance will not be an indication of future performance for organisations that have not developed sound plans and provided for appropriate resources to carry them out.

14. The costs that the banking industry will need to incur to address the Year 2000 are extensive. The Gartner Group has publicly estimated that it will cost between US$300 – US$600 billion worldwide just to complete needed changes and testing. Every line of code in every program needs to be reviewed at costs typically estimated at about US$1 per line. costs for global banks are frequently estimated in the hundreds of millions of dollars. Smaller banks with few in-house developed applications will still incur substantial costs to test thoroughly applications modified by others.

15. Skilled technical resources are already scarce and will become even scarcer as the deadline approaches. Already salaries for certain specialists are rising and key staff are being bid away by other companies. Consultants with top reputations are accepted only on a very selective basis. As time passes, banks will be forced to turn to consultants with little or no demonstrated performance record and uncertain futures.

16. Test facilities also can pose a challenge. Establishing a test environment for live testing using dates in the year 2000 is not easily done. If possible, dedicates systems should be used. Alternatively, a production system might be shut down and re-established for the Year 2000 testing, but such an approach can pose significant risks because moving an advanced date backwards (i.e. from 20xx to 19xx) for the operating systems is often a difficult and time consuming process. Also the number of weekends and holidays available to conduct testing is constantly shrinking. Renting computer time from third parties service providers may be possible but like consultants, their resources are being booked rapidly.

17. Testing will also be more difficult than usual. First, there will be competing demands for test environments. New applications like those related to the Euro or replacing fractions with decimals in trading activities will require testing in current environments. Yet given the importance of these applications and their interdependencies with other applications that must be tested for Year 2000 compliance, strategies will have to be developed for testing in both current and Year 2000 environments. Test data will need to be specially developed. Because testing is primarily a business line activity, business line resources will be under heavy pressure.

18. The Year 2000 is sufficiently complex that it should not be combined with other maintenance or software changes in the application. If problems are encountered, determining whether the Year 2000 or other changes are causing the problems can become extremely difficult. Many organisations are freezing other projects until the Year 2000 is addressed to minimise difficulties in tracking problems although such freezes are probably impractical for long periods of time.

Appendix B

Action Plans for Managing the Year 2000 Process in More Detail

Developing a strategic approach

1. Making sure that an appropriate strategic approach is developed by determining how best

to achieve Year 2000 compliance within an Institution's organisational structure represents the first phase. This phase includes an initial, high level sizing of the issue and developing a plan as to how best introduce the process throughout the organisation. This phase often relies heavily on technical staff knowledge of how information systems and technology are deployed and how business units are organised and interact with limited contact with business line areas. During this initial planning process, particular attention should be paid to assuring that during the organisational awareness phase, business lines will develop an understanding that the Year 2000 issue is not only a technical issue but a strategic one for each business line and that the business lines have ultimate ownership of the issue.

Creating organisational awareness

2. Making certain that the strategic importance of the Year 2000 as a business objective is understood and appreciated throughout the organisation may be the most important phase in the action plan. This phase has four basic objectives; creating visibility, ensuring commitment, identifying resources and formulating specific strategic objectives at a business line level.

3. Creating visibility throughout the business organisation is essential. Everyone must be aware of the potential problems posed by the date issue and become sensitive to applications where it might be an issue. Only in this way will all local applications be identified and addressed appropriately.

4. The recognition that the Year 2000 may be a survival issue requires a commitment from top management for its successful resolution as a strategic priority. Senior management and directors need to understand the issue and its implications and monitor progress on a regular basis. Specific responsibility for managing the issue should be clearly assigned. For larger organisations, a project office focused solely on the Year 2000 issue is recommended. Partnerships between technical staff and business lines must be developed with the business line managers accepting ultimate accountability to address the issue successfully.

5. Resource estimates need to be determined and built into budgets. Business lines need to recognise that testing will be the single most important resource intensive part of the project [4] and that responsibility for designing test plans and carrying out the tests rest with the business. Senior management must appreciate that operations and budgets. All applications throughout the bank must be addressed but some level of required maintenance and new product development must typically proceed.

6. Strategic decisions must be made at this stage because technology and business line resources will have to be redeployed. Opportunities exist to repair, replace, outsource or eliminate applications. Senior level guidance on how to make these decisions becomes critical.

Assessing actions and developing detailed plans

7. This phase moves the project from concept to concrete actions. Detailed inventories of what must be done are developed covering centralised and decentralised hardware, software and networks as well as equipment with embedded computer chips and logic. Particular care is needed to make sure that applications developed or procured locally at the business line level are included in the inventory. The inventories should include all aspects of business line

activities whether internal to the organisation or external to it. Risks should be quantified and priorities set based on these risks. [5]

8. Internal partnerships between technical staff and business lines should be solidified. The responsibilities of each should be clearly defined and timetables agreed upon. Producers for monitoring progress against schedules should be implemented with appropriate information flowing to senior management and directors on a regular basis.

9. Vendors and service providers should be contacted as to their status and plans for addressing the issue and contracts developed where appropriate. User groups can be helpful in making such contacts and getting information but are no substitute for an organisation following through with the information received. Applications must be able to work within the bank's own operating environment and responsibility for seeing that appropriate testing is done cannot be delegated to vendors or user groups. Making certain that current versions of software and operating systems are in place is particularly important because compliant applications may not work properly in a dated environment.[6]

10. Vendor management requires special attention and represents a continuous challenge throughout Year 2000 projects. Obtaining meaningful dates for product delivery, testing or other milestones is often particularly difficult, as vendors are concerned about the legal liability that may be associated with representations that prove to be in error. Notwithstanding this difficulty, the development of effective communication channels with vendors is essential.

11. During the assessment phase, one or more applications might be made year 2000 compliant on an expedited basis. Such pilots will help staff develop a better understanding of the work that must be done and permit better plans and budgets to be developed. Also, automated tools that help identify where dates are present should be tested as to their effectiveness.

12. This phase also should include a review of legal obligations. In particular, contracts with vendors and service providers should be reviewed as to respective responsibilities of the third party vendor. Insurance policies should be reviewed to see how Year 2000 problems would be handled if problems were to be encountered under various scenarios.

13. The development of detailed plans for the entire project should be the principal end product of the assessment phase. These plans need to address not only the changes that need to be made but also lay out key milestones, test plans and communication channels. The plans need to deal with internally developed applications whether centralised or decentralised with service providers and vendors and with correspondents and customers. Responsibilities and accountabilities need to be clearly defined for each step in the plans. The critical path within the overall plan needs to be determined; recognising that there will be many interdependencies that must be tested together.

Renovating systems, applications and equipment

14. Renovating systems, applications and equipment is the only phase of the process that is primarily technical. During this phase, the additional resources needed for the project should be acquired or contracted. Operating systems, applications, hardware and equipment needing

fixing should be modified, replaced, outsourced or discontinued. Automated tools and outside consultants probably have a role to play in most organisations during this phase.

15. In depth communication with vendors and careful monitoring of their progress occurs during this phase. In particular, a clear understanding of what the vendor means by being Year 2000 compliant must be obtained. This includes detailed knowledge of any environmental assumptions and planned changes in communications protocols. Agreement must be reached regarding the level of assistance the vendor will offer if problems are encountered. While a warranty or certification may be sought or offered the bank must recognise that such certification will almost certainly not cover interfaces with other applications and that the need for rigorous testing is not obviated by such a warranty or certification.

16. Identifying alternative approaches if renovations lag or fall is an important part of this step. Again, such contingency plans should deal not only with internal renovation work but also address the work of vendors and service providers as well as correspondents and customers with whom the institution interfaces. Contingency plans must include critical milestones for measuring progress or critical delivery dates where decisions must be made to pursue an alternative solution if the objective is not met. contingency plans need to take into account the mission critically of applications because, in all likelihood as the time certain deadline approaches, it will become impossible to fully implement all changes for all applications. Contingency plans need to recognise that in some cases, correspondent relationship may need to be altered or customer relationships served.

Validating the renovation through testing

17. Testing represents the largest single task in the Year 2000 project. Detailed test schedules must be developed and coordinated with correspondents and customers, particularly with an ever-decreasing number of weekend testing opportunities available. Full validation requires that Year 2000 data conditions be simulated for all elements of the test. Data flow internally and with third parties must be thoroughly tested while both the sender and received simulate Year 2000 conditions. Institutions need to participate in tests with service providers both on a bilateral test basis and in multi-user tests, which simulate full production volumes. contingency plans need to be implemented as needed when renovations are completed by specified cut-off dates.

18. During this phase, support facilities to assure that new or modified applications run properly are also developed. In particular, procedure manuals are written or rewritten and disseminated, training programs provided and help desks established or retrained.

Implementing tested, compliant systems

19. Implementation requires careful planning to make sure that interrelated applications are coordinated as to when they go into production. Coordination becomes particularly important when files at interfaces are changing in format. While recognising that coordination is necessary, putting compliant applications into production at the earliest possible date simplifies future testing.

20. The implementation phase also required monitoring of progress by service providers and vendors. Service providers in particular are likely to have two or more versions of an

application at any one time in order to meet the needs of institutions in various stages of implementation.

21. The implementation phase also includes reverting to contingency plans when necessary.

Appendix C

Checklist for a Successful Year 2000 Program

Building a successful Year 2000 program requires that a bank addresses a number of key factors and takes appropriate steps to address them. These factors include:

- Top Management understanding and endorsement as a strategic priority.

- Line management appreciation that it is not just a technical issue but potentially one of business survival.

- Explicit assignment of responsibility for the Year 2000 project and empowerment to carry it out.

- Detailed planning with the recognition that testing will be the most resource intensive part of the process.

- Appreciation that external testing may be among the most difficult parts of the process.

- Recognition that vendors and service providers cannot certify that their products will work properly with a bank's own applications, equipment and operating environment.

- Proactive communication with external vendors and service providers, and correspondents and customers.

- Prioritisation of applications as to their strategic importance.

- Identification of explicit resources to address the Year 2000 issues consistent with business priorities.

- Establishment of explicit target dates for milestones and regular reports to top management of progress.

- Active involvement of audit in the Year 2000 process.

- Clear contingency plans with trigger dates and procedures for implementation.

- Strong monitoring of security controls throughout the process.

---

2. Under current calendar conventions, years ending in 00 are generally not leap years, even though evenly divisible by 4. The exception is for centuries that are themselves divisible by 4. Thus, 2000 represents the

exception to the exception regarding leap year determination.

3. If date ranges span more than 200 years (e.g. when birthdates are part of a database), windowing is not a feasible solution.

4. Consultants estimate that testing will constitute anywhere from 45% to 70% of total Year 2000 costs.

5. The risk assessment and prioritisation process is particularly important because, in all likelihood for some institutions, resource limitations and inevitable problems will mean that some applications will not be Year 2000 complaint when the century date change occurs.

6. For organisations that do not have maintenance contracts on some or all of their equipment or software, version release issues may significantly expand the resources needed to become Year 2000 compliance.