THE YEAR 2000

A Challenge for Financial Institutions and Bank Supervisors

Basle Committee on Banking Supervision
Basle
September 1997

The Year 2000
A Challenge for Financial Institutions and Bank Supervisors

FOREWORD

1. The Year 2000 poses a significant challenge for financial institutions because many automated applications will cease to function normally as a result of the way date fields have been handled historically. Failure to address this issue in a timely manner would cause banking institutions to experience operational problems or even bankruptcy and could cause the disruption of financial markets. As a result, banking institutions must take the necessary steps to ensure that problems and disruptions are minimised.

2. This paper is prepared by the Basle Committee on Banking Supervision[1] in order to serve as a reference on the Year 2000 issue for central banks and other banking supervisors. It contains four parts that: (i) put the issue in perspective; (ii) outline the steps institutions need to follow to resolve the problem; (iii) discuss key issues that need to be addressed to resolve the problem successfully; and (iv) identify how bank supervisors can help assure success. A more technical and detailed discussion of the Year 2000 issue is provided in Appendix A. Appendix B describes the components that go into a successful action plan. Appendix C provides a short checklist summarising some of the key factors that banks must address to successfully meet the Year 2000 challenge.

[1] The Basle Committee on Banking Supervision is a Committee of banking supervisory authorities which was established by the central bank Governors of the Group of Ten countries in 1975. It consists of senior representatives of banking supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom and the United States. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat is located.

I. THE YEAR 2000 IN PERSPECTIVE

3. Banks rely heavily on automation to manage information. If automated applications failed to work properly, it would be difficult if not impossible to conduct business. While the Year 2000 problem is often seen as a technical issue, it is much more than a technical one because of the implications that not dealing with it properly could have on each and every business line within the bank. Every manager must be actively involved in assuring that the business line is Year 2000 compliant. Top management needs not only to recognise the strategic importance of the issue but also to monitor plans and progress actively across the bank.

4. The Year 2000 is particularly challenging because it is not just internal to a bank. Banks have many automated linkages and interdependencies with correspondents and customers. For larger banks that deal in multiple currencies and provide wide ranges of products in many countries around the world, the challenge is particularly great because many of these applications are interdependent. If applications are not able to work together properly, significant problems could develop. All of these interdependencies must be addressed and tested to assure that problems are not present. Similarly, banks rely on third party service providers or vendors for many applications. These applications not only need to be made compliant but also must be thoroughly tested within each bank to assure that they perform properly for the particular environment and application interfaces found in each institution.

5. Complicating the resolution of the Year 2000 issue on a global basis are the differing situations found in many markets and countries around the world. The scheduled introduction of the Euro is placing significant competing demands on scarce technical resources for institutions active in that market. Other new or modified financial trading or delivery systems are being introduced in other markets. In some countries, other policy or business objectives may divert technical resources from the financial sector. Even within the financial sector, there are differing priorities for banks, securities firms, and insurance companies. These and other factors lead to widely varying amounts of attention being devoted to Year 2000 issues by individual institutions.

6. Since the earliest days of electronic computers, programmers have used two digits to represent the year in date fields (YYMMDD). In the 1960s when this convention became standard, the two-digit representation made economic sense because it economised computer memory and saved storage space. Even in the 1980s, few believed that applications being developed then would still be running into the year 2000. Unfortunately, this belief was ill founded. While many newer applications are Year 2000 compliant, many older applications upon which compliant applications depend or interact continue to run. In addition, the environmental software and hardware on which an application runs may not be compliant.

Assuming that any application is Year 2000 compliant without appropriate analysis and testing poses substantial risks.

7. The Year 2000 problem exists because a two-digit representation of the year will be interpreted in many applications to mean the year 1900, not 2000, unless the date or program logic is modified. Many calculations will either indicate that transactions have been open for nearly a 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. These and other logic issues have the potential for causing problems for debt collection, ageing of information, calculating interest rates, etc. and could significantly disrupt normal business operations. Also, when dates are compared, customer billings may change from charges to refunds and vice versa. Even building systems such as elevators or climate control systems may be affected because of embedded logic to facilitate maintenance and operations.

8. All of these factors make the Year 2000 a formidable challenge. Whether the banking industry has the ability to rise to this challenge and avoid serious problems as the date change occurs will be determined by the actions that individual banks and the banking community more generally take between now and the Year 2000. To delay work on the issue runs the risk that all of the code modifications, testing and other changes cannot be done in a timely manner. Unlike most projects involving technology, the time certain nature of 1999 becoming 2000 makes it impossible to delay the event and full implementation of corrective actions.

II. ACTION PLANS FOR MANAGING THE YEAR 2000 PROCESS

9. All the indications are that achieving Year 2000 compliance will be both complex and resource intensive. Limited time exists and extensions are not possible because the century date change is a fixed reality. Detailed plans must be developed and resources identified and secured to achieve the objective. Organisations that are not well advanced in their Year 2000 efforts are going to be particularly challenged and will need to move quickly. All banking institutions need to assess where they and their correspondents and customers stand and to begin thinking about contingency plans.

10. Addressing the Year 2000 requires that every bank have an action plan. The complexity of the plan may vary from one bank to another depending upon size and the extent to which an organisation relies on outside vendors and service providers. However, even small banks with no internally developed applications must have a plan for dealing with the vendors and their equipment and systems with embedded chips. While individual organisations may have their own ways of describing their plans, one way to look at a good action plan is to think of it as consisting of the following phases. The specific actions to be taken in each phase are provided in more detail in Appendix B.

(a) Developing a strategic approach

11. This phase includes establishing Year 2000 as a strategic objective at the highest levels within the bank, developing a process to communicate the strategic objective throughout the banking organisation, and assessing the resource implications of the Year 2000 at a very high level.

12. At this time, organisations should be well past this phase in addressing issues.

(b) Creating organisational awareness

13. 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. The recognition that the Year 2000 may be a survival issue requires not only a visible commitment from top management for its successful resolution as a strategic priority but also an awareness of its importance by staff at all levels. Line management needs to understand the issue and its implications and accept ownership of the issue. Responsibilities should be clearly assigned. This phase have four objectives: creating visibility; ensuring commitment; identifying resources; and specifying specific strategic objectives at a business line level.

14. Organisations should also be past this phase in their Year 2000 project.

(c) Assessing actions and developing detailed plans

15. 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. The inventories should include all aspects of business line activities whether internal to the bank or external to it. Risks should be quantified and priorities set based on these risks.

16. While target dates for finishing this phase may vary from one country to another, organisations are expected to have completed this phase or be very close to completing it by September 1997 in many countries.

(d) Renovating systems, applications and equipment

17. This is the only phase of the process that is primarily technical. During this phase, the necessary fixing of operating systems, applications, hardware and equipment takes place. The development of contingency plans that identify alternative approaches if renovations lag or fail is an important part of this phase.

18. Organisations should be well into this phase at this time. Renovation work for significant applications that need to be tested with third parties must be completed with enough time to allow for thorough testing. In countries where Year 2000 preparations are well in hand, completion of this high priority work is being targeted for mid-1998. These countries also typically target that all renovation work be completed no later than the end of 1998.

(e) Validating the renovation through testing

19. Testing represents the largest single task in the Year 2000 project. Detailed test schedules must be developed and coordinated with correspondents and customers. Data flows, internally and with third parties must be thoroughly tested while both the sender and receiver simulate Year 2000 conditions.

20. In countries where Year 2000 preparations are well in hand, for at least larger institutions and all significant applications, the validation phase is being targeted for completion by the end of 1998. All validation work should be completed by mid-1999. Only with this schedule will there be sufficient time for industry and business wide testing with all correspondents and customers during 1999.

(f) Implementing tested, compliant systems

21. Implementation requires careful planning to make sure that interrelated applications are coordinated as to when they go into production. The implementation phase also requires monitoring of progress by service providers and vendors.

III. ISSUES

22. Addressing the Year 2000 represents a major and complex issue to manage. As organisations have developed their detailed plans, a group of issues have surfaced that deserve particular attention. While several of these issues have been discussed in describing the challenge and its management, they are highlighted in more detail here because of frequent misunderstandings or inadequate attention.

Certification

23. Certification has been a recurring and confusing issue for many institutions. Many institutions and especially smaller institutions believe that if a vendor certifies a particular product as being Year 2000 compliant, they need not worry about it. There are two fallacies to this idea. First, some vendors indicate that their product is compliant when in fact it is not. Second, even if the product is compliant, it still must be tested by the institution to make sure that it runs properly within the institution's own environment and interfaces properly with other applications. At least some level of testing by the business line area will be required to assure true compliance.

Vendor management

24. Third party vendors pose special risks because the amount of oversight and control that an individual bank can influence is limited. As a result, banks need to have a clear understanding of vendor plans and hold vendors accountable. If key targets are not met, contingency plans should be in place to change vendors, complete work internally, or otherwise adjust to vendor failure.

Target dates

25. Target dates for testing are critical both internally and externally. Most institutions have been developing target dates for testing for internal use but have not been active in communicating these dates to correspondents and customers. Because meaningful testing often requires testing internally and with external parties, the coordination of test plans with correspondents and large, active customers become very important to the institution. Indeed, setting priorities and internal target dates will depend to some extent on when external testing becomes feasible. Especially for larger institutions, payment systems, clearance and settlement systems, and similar utilities, communicating test plans for applications having external interfaces becomes crucial for the industry-wide planning process.

26. For institutions that may be somewhat lagging in their Year 2000 efforts to date, the need to communicate meaningful target dates for testing poses a dilemma. Not

communicating readiness dates for external testing now or indicating a date that is too far out in the future sends immediate indications to the financial community that the institution may be lagging in Year 2000 efforts. On the other hand, communicating a target date that appears acceptable but which might not be met runs the risk of having credibility questioned even more severely if the target is missed. Even internally, as institutions think about setting target dates for testing or other project milestones, they need to recognise that the century date change is inevitable. Setting optimistic targets that barely make compliance possible may be only disguising the real problem and issue for the organisation.

Spillover business risks

27. Spillover business risks and opportunities represent an area that is often overlooked when developing Year 2000 plans. Typically, institutions focus first on the internal efforts necessary to become compliant. Yet, the Year 2000 issue can also be a survival issue for customers. Failure of customers to make the necessary adjustments can lead to a loss of business and loss of asset values for the bank. On the other hand, having a strong Year 2000 program may open strategic opportunities to market the readiness posture of the institution. In any event, credit and relationship officers should already be cognisant of their customer's readiness, tracking progress over time, estimating possible business ramifications if customers fail to become compliant, and developing contingency plans as appropriate.

Mergers and acquisitions

28. Mergers and acquisitions represent another area where Year 2000 readiness should be taken into account because such activity would place additional burden on scarce technical and managerial resources of the organisations. At minimum, a rigorous due diligence on Year 2000 preparedness should be conducted in order to assess the status of the institution being absorbed and how the combined institutions would affect Year 2000 plans, actions and ultimately readiness. For organisations that are stretched in meeting Year 2000 compliance, acquiring another institution would be highly risky. Indeed, the possibility of being acquired might be an approach to contingency planning. However, as time passes, there is decreasing ability for any organisation to absorb a non-compliant one and make the necessary changes before the century date change.

Satellite operations and foreign activities

29. Satellite operations and foreign activities pose a significant risk for many institutions. While inventorying mainframe and other applications under the control of a centralised information systems management may be relatively easy, departmental applications unknown to the centralised operation are increasingly common. Many of these applications are essential risk monitoring and business decision tools. Extra effort is needed to

identify these applications and make certain that they are compliant. Making business line staff at all levels aware of the Year 2000 issue is essential if problems are to be avoided.

30. Similarly, foreign and decentralised operations frequently have applications specific to the local market trading activity or the local currency. Staff in these locations are often not as aware of corporate issues like the Year 2000 as staff would be at the head office. As a result, the likelihood increases that applications - potentially significant ones - would not be picked up in the inventory or appropriately addressed.

Security issues

31. Security issues arise and will become more pressing as the urgency of the Year 2000 increases. Normally sound security controls may be relaxed as consultants and subcontractors for consultants undergo less rigorous background checks before being granted access to bank systems and records. Date dependent security applications may be turned off to facilitate testing. As businesses focus more on resolving interconnectivity concerns, resources normally focused on security controls may be diverted.

Cost control

32. Cost control represents a problem area for many institutions. In particular, the adequacy of budgets becomes an issue. Many organisations appear to be underestimating the costs of testing by not recognising that many tests will have to be performed multiple times as vendors change releases or operating system environments or applications change. Additionally, business line management often fails to recognise that the largest share of the testing burden will ultimately fall to them.

33. Technical resource scarcities are also getting worse with the passage of time. Institutions are already experiencing significant turnover of key staff as salaries are bid up ever higher in the market. Bonuses and special retention packages are being used in many institutions to address the turnover issue.

34. Outside consultants are facing similar demands resulting in higher costs. Here, however, the issue is not just cost but the quality (skill and integrity) of the consultant and the level of confidence one can have that the consultant will continue to exist if problems are encountered. As a result of all of these factors, many organisations are finding it necessary to increase budget estimates, sometimes several times and often significantly.

Monitoring

35. Monitoring Year 2000 progress should be a high priority for every institution. The role that the audit function plays in the monitoring process should be clearly defined, proactive, and clearly visible at the highest levels. Follow up on audit exceptions should be tracked carefully and on a timely basis. Control mechanisms need to be developed

specifically for monitoring Year 2000 progress and senior management and directors need to be monitoring progress on a regular basis as one of the highest priorities of the institution.

Potential systemic issues

36. Potential systemic issues need to be identified. The Year 2000 issue is not one that will present problems only to those who fail to rise to the challenge. For large banks and industry "utilities" that serve the entire banking community by offering services or products not readily available elsewhere, problems focused in a single location could rapidly affect others if payments fail to move as expected. Potential weak links in the payment chains need to be identified as early as possible with appropriate contingency plans developed and followed as necessary.

37. Credit issues with systemic implications can also arise if very large customers or classes of customers become unable to conduct business. Obligations may not be met and collateral values can deteriorate rapidly. While the systemic implications of Year 2000 credit issues may take somewhat longer to manifest themselves, they are nonetheless real.

Outside auditors and public reports

38. Outside auditors and public reports are likely to become an issue at the end of the current fiscal year for some organisations. In some countries like the United States, the decision has already been made that Year 2000 renovation costs must be accounted for in the year in which they are incurred. While the accounting profession is still debating whether such costs will have to be disclosed as a specific item, there is building consensus that organisations appearing to be unable to be Year 2000 compliant for material businesses or applications will have to have this risk specifically noted in certified statements. At what point such disclosure begins to be required remains uncertain.

IV. ROLE FOR BANK SUPERVISORS

39. Bank supervisors clearly cannot solve the Year 2000 challenge; only institutions can do that for themselves. However, bank supervisors can play a constructive role in a number of ways.

Promoting increased awareness

40. Promoting increased awareness of the issue is probably both the simplest and most effective role that bank supervisors can play. Identifying the seriousness of the problem through alerts or other public notices that are carefully balanced and factual has been used successfully in a number of countries. In some cases, these public notices have included helpful guidance on how institutions might effectively address the issue. Direct contact with industry groups or individual institutions can also be used to increase the awareness of senior management.

Establishing targets and benchmarks for the industry

41. Establishing targets and benchmarks for the industry is another way to help assure progress. While different market circumstances may suggest that such targets will differ from country to country, having clear expectations helps institutions develop their own plans and furthers opportunities for external test plans. Several countries have already offered such benchmarks for their institutions.

Industry-wide status assessments

42. Industry-wide status assessments on progress can also be helpful. Bank supervisors are uniquely positioned to know the status of progress in each institution. If issues develop in particular locations or with particular types of entities, judicious public observations on the general level of progress may encourage the reallocation of resources to Year 2000 projects in these sectors.

Proactive supervisory pressures

43. Proactive supervisory pressures directed at specific problems and institutions is the strongest tool available to bank supervisors. While banks are the only ones that can make their applications compliant, supervisors can heighten the level of attention Year 2000 issues are receiving within the bank through a variety of supervisory tools. If, despite all efforts of the supervisors, a bank or group of banks are going to have significant problems, the supervisors should consider what contingency plans are needed to deal with the consequences.

V. SUMMARY

44. The Year 2000 issue is potentially the biggest challenge ever faced by the financial industry. Every automated system including equipment with computer chips embedded inside is potentially at risk and must be analysed and renovated or replaced if needed. Unlike most automation projects that can be staggered as to schedule and delayed if problems are encountered, all critical renovations must be addressed at once with no possibility for extending roll out deadlines. If resources and time prevent some non-critical applications from being renovated, the implications of such deferrals should be thoroughly analysed. As individual applications are addressed, they will have to be tested. In an age with extensive linkages among applications and interconnectivity among institutions, the testing process is enormous because tests must be done repeatedly as new components become compliant. Institutions that are not already addressing the Year 2000 date change as a strategic priority need to focus on this challenge immediately.

September 1997

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 compliant, many older applications upon which compliant applications depend or interact continue to run. Assuming that any application is Year 2000 compliant without appropriate analysis and testing poses substantial risks.

2. Further complexities to the issue are introduced by other considerations such as the use of reserved values such as using 99 in the year field to indicate that a file should be saved forever, archived, or treated differently in 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 years under a specified number (say 60) as being 20yy while years 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

[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 100 years (e.g. when birthdates are part of a database), windowing is not a feasible solution.

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 a 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 alone 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 more scarce 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 heavily committed, and new clients 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, dedicated 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 system 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 becoming Year 2000 compliant can rarely be achieved as part of normal business 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. Procedures 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

[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 compliant when the century date change occurs.

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 bank and 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.

[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 compliant.

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 fail 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 criticality 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 relationships may need to be altered or customer relationships severed.

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 flows internally and with third parties must be thoroughly tested while both the sender and receiver 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 requires 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 address a number of key factors and take 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.
- Recognition that correspondents and customers pose credit and other risks and analysis of the risks posed.
- Prioritisation of applications as to their strategic importance.
- Identification of explicit resources to address the Year 2000 issue consistent with business priorities.
- Establishment of explicit target dates for milestones and regular reports to top management on 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.