

Testing for Year 2000 Readiness

JOINT YEAR 2000 COUNCIL

**Basle Committee on Banking Supervision
Committee on Payment and Settlement Systems
International Association of Insurance Supervisors
International Organization of Securities Commissions**

Bank for International Settlements

September 1998

Testing for Year 2000 Readiness

Testing is consistently identified as the cornerstone of a successful Year 2000 program. Many sources indicate that resources required for testing typically make up more than half of total project costs. Only through a sound testing program can financial institutions be assured that their Year 2000 preparations have been thorough and that significant problems will not develop either internally or with key business partners. Many basic principles for successful Year 2000 testing will apply to all institutions. However, important differences in testing strategies will exist from organisation to organisation and market to market depending upon business priorities, complexity of operation, reliance on third-party service providers and vendors, and available resources.

Testing strategies for an individual institution or market is ultimately a business decision – what are the business risks faced if an application does not work, and what resources are appropriate to apply to reduce these risks to an acceptable level. For organisations starting late in their Year 2000 preparations, sufficient time and resources necessary to complete optimal testing may not be available. Business decisions and hard choices will have to be made on what is tested and how it is tested. Testing strategies need to be realistic and feasible and to make business sense for the organisation and for the market. Regulators and participants need to adopt strategies that are pragmatic and achievable lest resources be used in suboptimal ways.

This paper identifies the goals of Year 2000 testing, the elements that can make up a successful testing program, and the key factors that need to be considered by financial institutions in developing their own testing strategies.

Goals of Testing

The ultimate goal of the testing phase in Year 2000 programs is to ensure the operational integrity of systems and interfaces after remediation is complete. Testing as early as possible also identifies problems and maximises the time to fix them. Internal testing assures that applications and the software and hardware environment in which they run perform correctly and interact properly. Thorough internal testing is critical for every application and system that is essential for a business to function.

External testing focuses on the ability to conduct business normally with service providers, counterparties and customers. It provides an opportunity to focus on possible problems caused by systems and business partners that interface with an institution for which information on Year 2000 progress may be limited. For example through external testing, payment systems are able to observe which participants are not testing and where there may be unexpected or larger than expected problems. This knowledge permits appropriate contingency plans to be developed and implemented. Establishing testing milestones has the added advantage of bringing discipline to the market to ensure that prudent regulatory or other targets are being addressed appropriately. Where regulators and operators of exchanges and clearing and settlement systems see testing targets being missed, the denial of access to specific services or even regulatory action may be considered.

In addition to the direct consequences of testing, several broad goals may be achieved including the following:

- **Business continuity** – Year 2000 risk has the potential to impair the ability of entities to do business, especially those that rely on date-sensitive activities and processes. Where a large portion of business activities and processes depend heavily on technology, failure to test for Year 2000 readiness could have broad implications for the functioning of business enterprises.
- **Market stability** – Financial markets and payment and settlement arrangements rely on the orderly flow of information, often from parties around the world, to function properly. The interconnected nature of securities transactions and systems for trading, clearing, exchanging market data, and payments form the basic infrastructure of the financial market. The Year 2000 problem threatens to impede that flow of information by corrupting the information technology systems (*i.e.*, hardware and software) that make the information exchange possible. Unless payment and settlement arrangements successfully test for Year 2000 readiness, for example, the potential is high that there will be significant delays in settlement that could, in turn, have broad implications for financial markets more generally.
- **Public confidence** – If Year 2000 issues are not addressed properly, public confidence in financial institutions could be undermined, particularly if the media sensationalises the potential problems that could develop. Successful testing can offset or even pre-empt adverse media attention by indicating that dire predictions may be overstated.
- **Legal risk mitigation** – The failure to deal properly with the Year 2000 issue introduces the possibility that financial institutions may face legal liability to customers and counterparties who demonstrate damage from the failure to complete transactions normally. Testing strategies appropriate to the perceived business risk may be a way both to avoid problems and to mitigate claims of not taking prudent business precautions. From this perspective, testing should be both comprehensive and transparent.
- **Contingency planning** – The potential problems that could develop from failure to deal with the Year 2000 issue properly are so numerous that it is virtually impossible to develop effective contingency plans for all possible problems. Testing will help identify those vulnerabilities that are most likely to occur allowing resources for contingency planning and implementation to be deployed most effectively.

The diverse combination of goals that come out of the testing process underscores that testing is not simply a technical issue but rather one that requires the full attention of business managers. Effective testing strategies must be designed and executed by these managers who fully understand the underlying business risks. Failure to have active business commitment to testing almost assures that one or more of the goals of the testing process will not be met as effectively as they might.

Testing Elements

While every financial institution and market is different and testing needs to be adapted to address these differences, certain basic testing concepts should be borne in mind when devising testing plans. If tests are conducted in a hardware and software environment where all of the components are not yet Year 2000 compliant, tests should be repeated when components change. Some of the key testing concepts follow.

Internal tests are tests over which the testing institution has full control and in which external parties (customers, counterparties, and financial infrastructure operators) are not directly involved. Well-designed and thorough internal tests are the most important part of a successful test strategy.

- **Baseline tests** are performed before any changes are made to a computer program or application. The baseline test helps a financial institution compare performance of the system after changes are made to it in order to benchmark not only results but also operational efficiency.
- **Unit tests** are performed on one application to confirm whether remediation efforts yield accurate results for that application. They do not test how well the application will perform when it interacts with other applications.
- **Integrated tests** are performed on multiple applications or systems simultaneously. Integrated tests confirm whether computer programs function properly as they interact with other programs. Integrated tests should be repeated when the operating environment changes.¹
- **Future date tests** simulate processing of renovated programs and applications for future critical dates to ensure that those dates will not cause program or system problems. Specific dates to be tested will vary depending on the application. For applications that will be running at the century date change or across multiple time zones, testing while the date rolls over will be necessary. For all applications, testing for the first business day in 2000 is essential. In addition, there are a number of other special dates such as leap year rollover in 2000 that may warrant testing.²
- **User acceptance tests** are performed with internal users and validate whether the remediations have been done correctly and applications still function as expected. Internal user acceptance may often be part of integrated and future date tests.

¹ Where integrated tests have been successfully completed and the operating environment changes, it may be possible to avoid repeating unit testing if an integrated retest is successful. However, if problems are identified, unit tests may be necessary to identify the source of the problem.

² A list of key dates that have been identified as being potentially problematic is provided in the Annex. It is unlikely that all of the dates listed in the Annex will need to be tested, but business managers should evaluate the risks associated with the particular dates in developing appropriate testing strategies.

External tests are conducted by an institution to assess the risks in remediating and internally tested systems where they interface with systems and applications of other institutions and systems. In most instances, external tests will be coordinated with the external party. External tests are particularly important where the interfaces are proprietary or specific to the particular business activity or service provider and the external dependency is mission critical for the business activity.³

- **Point-to-point tests** verify the ability of a financial institution to transmit and/or receive data with another entity or system. Point-to-point testing is the simplest form of external testing.⁴ Particular care is needed to verify that dates are synchronised for all systems involved in the test. Point-to-point tests are particularly important in all instances when the file format for communication is changed.⁵
- **End-to-end tests** verify the ability of a financial institution originating a transaction to transmit test data to a receiving entity or system through one or more intermediaries performing business functions and to have applications achieve the desired results.^{6 7} End-to-end tests are particularly appropriate for real-time, interactive applications. Participants will typically share test scripts⁸ before testing.
- **Street-wide or industry-wide tests** permit most or all participants to test simultaneously to simulate actual business activities for a particular application, product or market more realistically.⁹ Such tests are typically scheduled cooperatively by industry groups or by governmental bodies. Agreed upon test scripts are typically used for such tests.
- **Beta tests**, as used in the context of Year 2000 testing discussions, are limited participation external tests that are designed to assure that test scripts achieve the desired results. It is not unusual for scripts for beta tests to be modified based on initial test results before being adopted for broader use.
- **Tests with monitoring** are often used by exchanges, clearing houses, payment systems, and other financial institutions that are essential to the infrastructure of financial markets. Monitoring permits the service provider to determine the participants that are conducting tests with it. In extreme cases, the service provider may establish target dates and standards that must be met by participants to qualify for continuing access to the system.

³ As a practical matter, service providers may not be able to provide testing to every client. However, if the service and interface provided is exactly the same for all clients and is unchanged in the mediated application, testing with a subset may provide reasonable assurance that all clients that have tested internally will be able to function normally.

⁴ Point-to-point testing may also be used to refer to internal tests between different business units or applications.

⁵ If a file format changes after external testing is completed, the tests should be repeated.

⁶ End-to-end tests are sometimes referred to as multilateral tests to distinguish tests that are among intermediate processors testing among each other without including the true end points of a transaction.

⁷ End-to-end tests are not typically designed to test telecommunications and other infrastructure providers.

⁸ Test scripts are documents describing the testing procedures and the events to be tested.

⁹ Street-wide or industry-wide tests are often designed to test all business functions but at lower than normal volume levels in order to avoid overloading test environments. The design of such tests is typically a resource intensive activity. The realistic ability to conduct such tests will decrease as Year 2000 approaches.

- **Tests with monitoring and affirmation** are used by some institutions essential to the infrastructure of financial markets for the participants that are also deemed to be part of the infrastructure. In this instance, not only is the participant's testing monitored, but also the participant is asked to have a responsible official certify that the test was indeed part of an overall business process test.
- **Proxy tests** are tests conducted by a third party as an alternative to testing by an institution itself. Proxy tests are often conducted by user groups as an alternative to each member testing separately. Because every processing environment and the procedures in place for its operation will have unique elements, reliance on proxy testing is an imperfect substitute for an institution or user group actually conducting the test itself. However, proxy testing may be appropriate when it is not practical for every user of a service to conduct point-to-point or more complex tests with every other user of the service. Proxy testing is also helpful in setting priorities. For example, if one or more institutions have successfully tested a product, other institutions using that product might consider testing it a later date in order to focus on higher priorities. Also, for organisations with limited resources or insufficient time to complete testing, proxy testing may be the only alternative. Proxy tests should not be considered as an adequate substitute for a well designed test program and should generally be discouraged when more complete testing is feasible. Proxy tests should not be used by providers or clearing or payment services upon which many other institutions depend and for which no acceptable alternative exists.¹⁰
- **Cross-border industry tests** are designed to allow more realistic testing of financial systems connecting different countries.¹¹ Cross-border tests are effectively industry-wide tests in which major payments systems and/or exchanges and clearing houses operate in a synchronised, future dated environment in two or more countries in order to simulate normal business days. In many instances, multiple time zones will be involved requiring special attention to ensure that not only calendars but also clocks are set properly. Efforts to organise such tests are only recently getting underway.

This listing of the various types of Year 2000 tests is approximately the order that many organisations will consider conducting the various tests. However, the ordering and the relative importance of each type of test will vary from application to application and from one organisation to another. Therefore, each organisation needs to determine its testing strategy for itself including what tests are necessary and the order in which tests should be conducted.

Factors to Consider in Developing a Test Strategy

Developing effective test strategies for Year 2000 requires institutions to balance a number of business objectives and risks and recognise resource and time constraints that they may face. Additionally, external elements are to be taken into account. They include third-parties support for business operations, Year 2000 readiness of customers and counterparties, and their likely impact on normal business operations. Understanding test plans for external

¹⁰ While a service provider of a critical infrastructure application should avoid relying on proxy testing for all components of the application, users of the service that rely on standard access tools may find that proxy tests of these tools are acceptable.

¹¹ Financial institutions that deal in multiple currencies or in assets from multiple jurisdictions may also be engaged in bilateral cross-border testing with counterparties in multiple jurisdictions. This concept is separate from cross-border industry tests, which are industry-wide.

bodies is essential in order to develop test strategies that allow appropriate coordinated external testing.

- **What is important and feasible?** As the century date change approaches, it will be increasingly difficult to renovate and test all applications and systems. Several leading technology consultants already predicts that many major organisations – both financial and non-financial – will not be Year 2000 ready for at least some non-mission critical¹² applications. A significant number will not be fully ready for some applications deemed mission critical. For many of these major organisations, choices will have to be made regarding what should be tested since not enough time exists to test everything. Smaller institutions facing apparently lesser challenges may have also to make similar tough choices on testing.

Identifying those business operations that are essential for business viability is critical. Establishing priorities for testing consistent with those activities that are truly essential will maximise the likelihood that both testing and the Year 2000 program will not fail.¹³ In many cases, difficult business decisions will have to be made, particularly as time becomes even shorter.

- **What resources will be available for testing?** Testing is resource intensive and requires business knowledge. It requires not only technical resources in the form of a test environment¹⁴ and technical staff to run and monitor it but also business resources to design appropriate tests and participate in the test itself.

For many system changes, it has been possible to hire outside consultants to handle technical tasks and purchase time on test systems to conduct tests. As the Year 2000 approaches, however, such outside assistance, especially with the necessary business knowledge, is becoming increasingly difficult and expensive to acquire. Making certain that managers, technical staff, hardware (including staff to run it), and business personnel to oversee testing are available needs to be a very high priority in developing a testing strategy. Establishing an aggressive test strategy but not having the resources to complete it may increase overall business risk if too much resources are devoted to secondary tasks and key tests are unable to be performed.

- **How complex are business processes?** Organisations that have essential business activities that require real-time, interactive processing with counterparties and customers generally should have testing programs involving end-to-end testing and, in

¹² “Mission critical” systems are those that a financial institution needs to have operational in order to conduct its most basic functions (*e.g.* execute payments). As part of developing a detailed inventory of applications during the assessment phase, each institution should rank the risk associated with an application not functioning properly. The applications with the highest risk rankings are those that are mission critical.

¹³ Experience shows that some of the more complex forms of testing (*e.g.* end-to-end, industry-wide testing) require significant time and resources for their design and execution. Considering the time and resource constraints that prevail, clear testing priorities must be established with a view to minimising any potential risk of disruptions.

In some instances, testing may not be feasible such as with “no alternative” telecommunications or utility providers that provide no or very limited testing opportunities. In these circumstances, institutions should focus on testing the customised aspects of their interface with such service providers, in conjunction with strong due diligence on the preparations of the service provider and contingency planning.

¹⁴ Obtaining an appropriate environment for testing is becoming increasingly challenging as weekends and holidays diminish and third-party sources become fully booked. Even large organisations that have invested in dedicated test environments are facing problems when different markets or products schedule mandatory tests on the same day but with different test dates.

many instances, some type of industry-wide testing, if such testing is feasible. For other applications, which do not involve real-time and interactive processing, organisations may provide counterparties or customers with instructions and information and wait for the other party to execute batch-type processing at periodic intervals. In these instances, it may be possible to rely more heavily on more simple point-to-point tests as long as the ability to retrieve return responses in a timely manner is also tested.

Recognising what type of test is necessary for meaningful testing of business activities and designing test strategies accordingly is essential for effective resource utilisation.

- **Do meaningful alternatives exist?** For some business functions like clearance and settlement, no meaningful alternative exists to the use of the external system. For example, the inability to interact properly with an exchange, clearing agency, or payment system may not allow transactions to be conducted without undue delays and serious financial consequences. For these external systems for which no acceptable alternative exists because of the transactions volumes or other factors, testing at the most rigorous level is essential. In these instances, the only contingency plan may be to test, and retest again. The “no alternative” service provider that serves as a conduit for financial transactions bears a special burden to see that participants are sufficiently prepared as to avoid system disruptions.¹⁵ Typically, such organisations will rely on monitoring or monitoring-with-affirmation as a means to assure that systemic problems do not develop with the century date change.

In other instances, where an alternative service provider may be readily available, the need for rigorous testing may be somewhat reduced. In these cases, however, it is important to test thoroughly the proposed alternative to make sure that contingency plans that permit processing along the alternative route have been thoroughly validated for volumes as well as functionality.

Distinguishing between what must be tested and what should be tested and allocating testing resources accordingly will become an increasingly critical decision as time becomes shorter.

- **How structured should external testing be?** Regulators, trade associations and individual service providers often establish targets for certain types of tests or even specific schedules for mandatory testing. Such tests may also have detailed scripts for participants to follow. In other cases, service providers may offer test environments and leave it largely up to the participant, counterparty, or client to design their own testing plans.

Those establishing target dates or schedules for coordinated tests or developing test scripts should take care to make certain that the targets and plans are realistic for the market. Unduly aggressive targets that cannot be met by significant numbers of participants without their reallocating significant test resources should be avoided. Also, very complex test scripts that require substantial resources to develop and

¹⁵ Participants in payments or clearance and settlement systems are unlikely to be able to test with every other participant. Operators of such systems will need to design test strategies in ways to assure that participants can reasonably assume that they can conduct transactions with the entire participant community if they have participated in appropriate tests.

execute could result in institutions adjusting priorities to the detriment of overall business and broader financial market risk.

Annex

Key Year 2000 Test Dates

The dates for which an institution will want to test will depend upon the application, the market, the perceived business risk associated with a particular date, and the available resources. The following list includes many of the Year 2000 related dates that organisations have identified as being important for testing in at least some applications. Other dates may be important for specific products or markets. Many of these dates may be appropriate for internal tests but unnecessary for external tests. Others may not be tested at all because the business risk does not warrant it or because higher priorities and limited resources do not permit such tests. In some instances, institutions will want to test the “rollover” into or out of particular dates.

Date	Reason
April 9, 1999	9999 on the Julian calendar. ¹ In many computer programs, 9999 denotes “end of input.”
September 9, 1999	9999 on the Gregorian calendar. In many computer programs, 9999 denotes “end of input.”
December 30, 1999	Last business day in 1999 for many markets.
December 31, 1999	Last day in 1999 year.
January 1, 2000	Beginning of Year 2000.
January 3, 2000	First business day in 2000 for many markets.
January 4, 2000	First business day in 2000 for many markets.
January 10, 2000	First business day to require 7 digit date field (10/1/2000)
January 31, 2000	End of first month of 2000.
February 29, 2000	Leap year day. ²
March 31, 2000	End of first quarter of 2000.
October 10, 2000	First date to require an 8 digit date field (10/10/2000)
December 31, 2000	End of Year 2000.
January 1, 2001	Beginning of Year 2001.
December 31, 2001	Check that year has 365 days.

¹ Although the Gregorian calendar is used throughout much of the world, some computer programs are based on the Julian calendar.

² The Gregorian calendar does not have leap years in years that end in xx00 except when xx00 is evenly divisible by 400. Thus, 2000 is the exception to the exception regarding leap years.