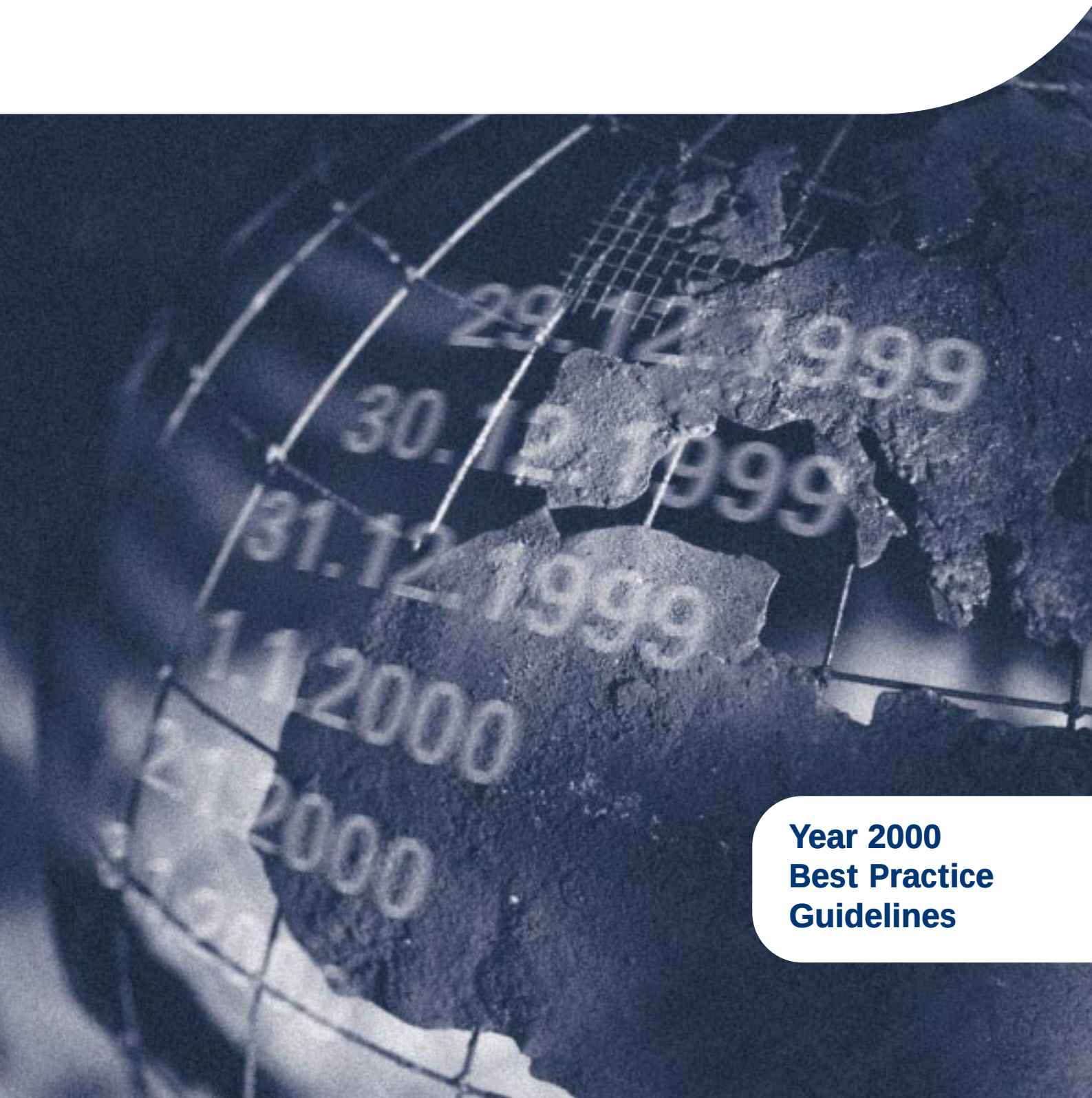
FOA
THE FUTURES AND OPTIONS ASSOCIATION



Year 2000 Best Practice Guidelines

The Futures and Options Association

The Futures and Options Association (FOA) is a London based trade association representing firms, institutions and exchanges involved in futures and options business.

It undertakes a variety of activities ensuring that the commercial environment in which members carry on their business is appropriate and cost-effective for the use of derivative products

The FOA has an international membership of 200 banks and other financial institutions, commodity trade houses, fund managers, corporate treasuries and specialist firms which provide legal and accountancy services to market participants.

For further information contact: Lucinda Campbell-Gray, Director of Operations
The Futures and Options Association
One America Square
17 Crosswall
London EC3N 2PP
Tel: 0171 426 7250
Fax: 0171 426 7251
www.foa.co.uk
E-mail: info@foa.co.uk

PINSENT • CURTIS

Pinsent Curtis is one of the UK's leading lawyers, with City and international expertise in securities, commodities, financial services, banking, corporate finance as well as Year 2000 and IT legal issues for the financial industry. Pinsent Curtis has acted as advisor on the FOA Year 2000 project.

For further information contact: Craig Hope, Partner
Pinsent Curtis
Dashwood House
69 Old Broad Street
London EC2M 1NR
Tel: 0171 418 7000
Fax: 0171 418 7050
e-mail: craig.hope@pinsent-curtis.co.uk

Foreword

Foreword

The new millennium is now little more than a year away. Financial firms and markets have been acutely aware of the Year 2000 risks for some time. So too have their regulators, both in the UK and internationally. The Bank of England is closely involved in a number of national and international efforts to raise awareness of the problem and ensure that issues such as testing and contingency planning are fully addressed.

Here in the UK, in our periodic "Blue Books", we have drawn together information about the many initiatives now in train. But the Blue Books, like much of the output of the international committees now active in the field, is necessarily high-level; it points to the areas where things are happening or need to happen, and provides a forum for discussion and debate, but it does not and can not provide a detailed route map. That very important work is for the trade associations, exchanges, system providers and individual firms, who know their markets and systems better than any outsider.

The Futures and Options Association's initiative in developing guidelines for best practice in dealing with Year 2000 issues, their organisation of an industry test in relation to London exchange-traded futures and options, and their development of a system for self-certification, are important and useful steps which the Bank whole-heartedly supports. The detailed procedures set out in this booklet are the fruit of much consultation and debate within the industry. They represent a clear statement of best practice which will, we believe, serve the industry well over the months ahead.

Alastair Clark
Executive Director, Bank of England

Introduction by: Sir Michael Jenkins, Chairman, FOA

"The Year 2000 problem is a business issue for virtually all regulated institutions. The responsibility rests squarely with their boards and senior management to ensure that their institutions identify and do what is necessary to achieve adequate business continuity".†

This introduction to the FSA's policy statement on Year 2000 makes it clear that regulators will be looking to senior management to give top priority and maximum support to Year 2000 projects within firms, and will be expecting them to report on progress and achievements.

In response, the FOA has prepared these guidelines which set out a common standard for the industry together with a scheme that allows firms to self-certificate using a recognised template. Once completed and signed off by the senior executive with responsibility for millennium issues, it is intended that the scheme will become accepted as demonstrating that a firm considers that it has satisfactorily reviewed its position in respect to the Year 2000; implemented any necessary remedial actions; tested and prepared an appropriate contingency plan. In other words, taken all reasonable steps to ensure they are properly prepared and "fit and proper" to continue trading into the next millennium.

By using these guidelines it is hoped that the London markets may demonstrate their stability to the rest of the world and contribute more generally to public confidence that the financial sector will be in a position to provide adequate business continuity into the 21st century.

Sir Michael Jenkins
Chairman, FOA

† FSA Policy Statement, October 1998

Contents

Contents

Introduction 6

The Guidelines 7

Certificate 13

Checklists

1 15
2 16
3 17
4 18
5 19

Appendix 1 21

Appendix 2 23

1. Introduction

The Year 2000 poses serious challenges to the derivatives industry. The majority of computer operating systems and programmes currently in use have been developed using six digit fields (yymmdd). Up to the end of 1999 this two digit date field will suffice, using a subtraction of current date from some future date. As the industry enters the year 2000, the two digit field “00" may not permit consistent calculations based on current formulae. In addition there are concerns whether software will take year 2000 as a leap year. The potential impact is that date sensitive calculations may be based on erroneous data and could cause a system failure.

Virtually all organisations may be affected in some way. Systems are often complex and have been developed over many years through a variety of computer languages and hardware platforms. Regardless of project size or complexity, strong leadership, effective communication and accountability are essential to ensure that Year 2000 initiatives are successful.

In any Year 2000 project it is necessary for a firm to consider all its businesses, processes and systems. Only following a full inventory and assessment can the impact of interdependencies and interrelationships in systems be identified and prioritised in relation to whether they are critical to the business (or businesses) of the firm.

The Futures and Options Association believes that there are tangible benefits to be gained by the adherence to an uniform standard to be applied in relation to London exchange traded futures and options. This set of guidelines, has been formulated by the FOA in consultation with its members, the London Exchanges , (IPE, LIFFE, LME, OMLX) and the London Clearing House. The guidelines are applicable to all the businesses conducted by a firm and require all the businesses to be assessed. In relation to businesses outside London exchange-traded futures and options, firms will have to establish or elect to perform relevant industry specific testing programmes.

While the FOA believes that successful completion of the programme contained in these guidelines represents best practice and reasonable steps that firms can take in relation to Year 2000 issues, there can be no guarantee that adherence to the guidelines and satisfactory performance of the tests will necessarily deliver Year 2000 conformity.

2. The Guidelines

2.1 The Standard adopted

In formulating these guidelines the FOA has adopted the standard Year 2000 conformity defined by the British Standards Institute technical committee (BDD/1/-3 reference DISC PD2000-1). (See Appendices 1 and 2 for detailed definitions).

"Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the year 2000".

In particular:

Rule 1: No value for current date will cause an interruption in operation

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

Rule 3: In all interface and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules

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

2.2. Responsibility

The Year 2000 is not just an IT problem and may have an impact on diverse areas of business. All businesses conducted by a firm need to be considered. The problem should be defined within each individual organisation and a Year 2000 Project Team, led by a senior level executive, either at board level or reporting directly to the board, partners or owners. Persons having responsibility and authority to make decisions that control elements of the year 2000 programme and processes should be identified and their responsibilities defined and documented. Responsibility means that the person has the necessary level of authority for making policy, setting objectives, planning implementation, reviewing achievements, and taking corrective action.

The Team should develop the firm's Year 2000 strategy which should contain a High Level Impact Analysis, and communicate it to relevant staff at all levels. This strategy should include reference to budgeting, staffing and overall time frames.

The High Level Impact Analysis needs to consider the risks and exposures to the firms' business or businesses, the potential impact of the year 2000 problem on business processes, and what they depend on. The Team therefore needs to be able to consider the impact on the businesses of systems, the effect on the firm's accounting and risk control systems, its reliance on third parties for information or processing and the interdependencies of internal and external systems. In addition the Team should contain

individuals with responsibilities for the resources needed to achieve the strategy. Within the Team individual responsibility should be allocated for IT, business areas, front office, back office, compliance, budget/finance and human resources. Internal and External Audit should also be involved.

The Team should regularly review resourcing to identify requirements and provide adequate resources including the assignment of trained personnel for the management, performance of work and verification, and to ensure the completion of tasks within timescales.

The Board should be regularly informed of progress and accomplishment to ensure suitability and effectiveness

See Checklist 1.

2.3. Assessment

A complete inventory of all systems and interfaces including hardware, software, networks, processing platforms, customer and vendor interdependencies should be completed in order to identify exposure and prioritise systems. This prioritisation will occur after risk analysis of the various systems has been conducted. This inventory should also include environmental systems dependent on embedded microchips e.g. security systems, lifts etc.

All programmes, routines, spread sheets and applications should be listed and described uniquely and should include links and interfaces with markets and outside third party organisations including service suppliers i.e. fax, telephone, electricity.

The systems software and hardware then need to be assessed in relation to whether they are prima-facia compliant or non-compliant to the Year 2000 Standard. The assessment should include consideration of relationships/third parties, vendors products and services that the institution uses, other financial institutions, clearing houses, exchanges and customers with whom it exchanges data electronically, and customers whose standing may be diminished by significant disruptions associated with the millennium change. The firm must make an inventory of all hardware and software.

The Team needs to consider which systems are business critical, considering both the potential damage that would be caused to the firm as regards failure of the system and whether failure of the system will prevent the firm from continuing business operations.. This involves reviewing the systems against the High Level Impact Analysis to determine business criticality. Systems should be prioritised for action in relation to their criticality to the business. Resources should be allocated in relation to necessary actions.

See Checklist 2

2.4 Repair/Replacement

Decisions on each inventory item must be made. Cost and timing may influence an organisation's decision to repair or replace business critical systems. These factors may dictate that some systems undergo short term repair and are replaced sometime after Jan 1 2000.

Execution should be done systematically with priorities set in accordance with risk, determined from the assessment phase.

The firm will have to establish in relation to outside suppliers whether their assurances (if any) are adequate, and where repair or replace is planned, consideration will have to be given for the need to use historical or archive data to run on the new compliant system. Consideration should also be given to the effect of repair or replace of particular systems impacting upon other systems with which they interface. Any repaired/replaced activity should be followed by full testing to ensure that the changes are effective and that the system's functionality has not been compromised.

All decisions to repair and replace should be fully documented and implementation properly controlled.

2.5. Validation

Thorough testing is critical to any Year 2000 project. The objective of testing is to ensure that all hardware and software, including that repaired or replaced, and including interfaces with other systems, demonstrates no Year 2000 problems.

The firm should develop a testing strategy and testing priorities based on the risks of the failure of the system that they have in operation, determined from the High Level Impact Analysis. Testing should relate to all those systems which are categorised as business critical which may include environmental systems, electricity, telephones etc. Business critical systems should be tested first.

Data and dates chosen for the test should relate to every significant business transaction, and encompass the relevant dates involved in a transaction, i.e. booking, settlement, occurring across the critical rollover dates. Critical dates may vary for firms depending upon the markets they operate in and the particular characteristics of those markets. The test environment should be an appropriate representation of the live environment.

Firms need to consider the types and extent of testing required. All systems should be internally tested to ensure that hardware, operating systems and applications demonstrate compliance with the Standard.

Where firms interface with infrastructure providers or institutions, e.g. exchanges and clearing houses, the firm can

- participate in a recognised industry test
- use canned data produced by an industry test as a feed into their internal systems
- opt to test by proxy (see over).

Industry tests consist of a group test of particular markets and systems. The FOA has recently co-ordinated a test of the London exchange-traded futures and options market and has published a catalogue of scripts performed by a beta group. Canned data relating to this test should be available in due course.

Testing by proxy is possible where tests have been carried out on a particular interface by other parties and a firm deems that the combination of systems and infrastructure involved was sufficiently close to its own configuration to negate the need for further physical testing of that interface. The firm must use its judgment as to how technically valid such a comparison is.

Firms should document their decisions on whether and how to test each interface.

See Checklists 3 and 4

(See Appendix 2 for detailed definitions of compliance testing).

2.6 Contingency Planning

Firms should produce contingency plans in relation to critical business systems, with a view to preventing and minimising impact, and to assure business continuity. These plans should also include major service providers, (including electricity, phones etc,) and should be tried and tested themselves. Some elements of contingency planning should be done at the assessment of Repair/Replace phase.

Contingency plans require the evaluation of the risks associated with the failure of a business-critical system. The plans should ensure that if the systems fail, there are back-ups to ensure that the firm continues to remain viable. Contingency plans should consider the status of Year 2000 readiness, renovation and replacement plans for business-critical systems, including those in relation to counterparties and third parties. They should also consider the financial and marketing impact of the loss of a critical business system and the impact of any regulatory requirements.

Contingency plans need to cover markets, third party suppliers, and counterparties, and may require the co-operation with these parties. Firms serviced by third parties should take into account the contingency plans of those third parties in their own contingency plans.

Contingency plans should be cost-effective, practical and appropriate for the size, complexity and type of information system used. This may involve consideration of whether a system could be replaced by a manual or automated process. The objective should be to minimise disruption and maximise speed of recovery.

Contingency plans should deal with how failures will be addressed in relation to interest penalties etc, in relation to its significant business clients, whether customers' assets can be identified and preserved and instructions can be accepted and executed. There should also be mechanisms in place for a fair and expeditious resolution of disputes with customers that may arise.

Plans should include the retention and preservation of information in machine-readable copies of the firm's master files and transaction files; printed or other similar medium such a microfiche file balances; electronic text format copies of all master files and file balance reports.

See Checklist 5

3. Self-certification

In order to self-certify, firms should have completed all checklists and in particular created and maintained full documentation reflecting completion of all steps in the guidelines. The checklists should be signed off by the Senior Executive with responsibility for Year 2000.

3.1 Documents

Firms need to establish and maintain procedures to document and control all decisions and data. This should apply to contractual documents and specifications, planning documents, documents evidencing decisions and changes to systems.

All documentation should be approved by authorised personnel prior to issue. There should be a master list identifying the current revision status of documents which should be established to preclude the use of obsolete documents. It may be necessary to retain obsolete documents for potential legal use. All actions and changes should be identified and tracked. A change management procedure should be adopted so that changes to documents are reviewed and approved by the same functions, organisations or individuals that performed the original review.

The firm should maintain records to provide evidence that the product has been tested. It should show clearly whether the product has passed or failed according to defined acceptance criteria. Records should identify the inspection authority responsible for the release of the system.

Records and documentation should be legible and should be stored and retained in such a way as they are readily retrievable. A retention time should be established and recorded.

Important

In issuing these guidelines and the tests together with appendices and other related documentation the FOA, its member firms, participant parties, LIFFE, IPE, LME, OMLX, the LCH, and Pinsent Curtis neither warrant nor represent, either expressly or impliedly, that satisfactory completion of the guidelines will ensure Year 2000 compliance. The Guidelines have been compiled on the basis that they reflect best industry practice and are believed to encompass reasonable steps, but no liability will accrue against the above mentioned parties whether in contract, tort or breach of statutory duty or otherwise in the event that Year 2000 problems occur.

Year 2000 readiness

<Company name>
<Address 1>
<Address 2>
<Address 3>
<Postcode>

<date>

To whom it may concern:

The above named firm has followed/is following the FOA Year 2000 programme as detailed in the published guidelines. The following sections have been completed:

- ☐ Responsibility
- ☐ Inventory and Assessment
- ☐ Internal testing
- ☐ External testing
- ☐ Contingency plans
- ☐ Further details may be found on the attached checklists
- ☐ Documentation on all aspects of our Year 2000 project is available

Name: .....Position: .....

Signed: ..... Date: .....

Checklist 1: Responsibility

	..... (Board member/Partner/Owner)	
..... (IT)	..... (Internal Audit)	..... (Budget/finance)
..... (Business)	..... (Back Office)	..... (Front Office)
..... (Human Resources)	..... (Compliance)	.....

The Year 2000 team report to the Board weekly ☐ monthly ☐ quarterly ☐ other: .....

The resourcing of the project is reviewed weekly ☐ monthly ☐ quarterly ☐ other: .....

A High Level Impact Analysis has been completed and the identified risks and exposures clearly communicated to all appropriate departments ☐

Full documentation on all aspects of the project is available for inspection ☐

Name: ..... Position: ..... Signed: ..... Date: .....

Checklist 2: Inventory and assessment

An inventory of all systems has been completed including

- hardware ☐
- software ☐
- networks ☐
- utilities ☐
- environmental ☐
- third party suppliers ☐

The inventory has been assessed ☐

A list of business critical systems which have been identified is attached ☐

Priorities have been set in relation to replacement/renovation ☐

Full documentation on all aspects of the project is available for inspection ☐

Name: ..... Position: .....

Signature: ..... Date: .....

Checklist 3: Internal testing

date tested	system	application	version	hardware	operating system

Unit and integration testing has been successfully carried out and all internal business critical systems, processes and procedures, as specified above, meet the identified Standard

Name: ..... Position: .....

Signature: ..... Date: .....

Checklist 4: External testing

All business critical external interfaces have been identified and tested as detailed below:

i) External integration testing (testing between A and B where A is the firm self-certifying)

Interface/systems	External Organisation B	Test Date
Example: Exchange feed to Back Office	Exchange	

ii) Point to Point testing (testing between A and C through B where A is the firm self-certifying)

Interface/systems	External Organisation B	External Organisation C	Test Date
Example: Exchange feed to Member Back Office via Bureau	Back Office Bureau	Exchange	

iii) Proxy testing (interfaces tested by third parties and considered to be Year 2000 ready)

Interface/systems	Third Party Test	Test Date
Example: Exchange feed to Back Office	FOA Beta test	October 1998

Full documentation of all tests detailed above has been completed and is available for inspection ☐

Name: ..... Position: .....

Signature: ..... Date: .....

Checklist 5: Contingency plan

trigger date	Scenario	risk prevention strategy	risk mitigation strategy	contingency plan	authority required

Potential outcomes that could have significant negative impact on our business have been:

identified assessed prioritised

For each of these potential outcomes:

risk prevention strategy is in place risk mitigation is in place

Full documentation on all aspects of the project is available for inspection

Name: ..... Position: ..... Signed: ..... Date: .....

Appendix 1

Appendix 1:

A definition of Year 2000 confirmity by the British Standards Institute Ref: PD2000-1

THE DEFINITION

Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the year 2000.

In particular:

Rule 1 No value for current date will cause any interruption in operation.

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

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

Rule 4 Year 2000 must be recognized as a leap year.

AMPLIFICATION OF THE DEFINITION AND RULES

1 General Explanation

1.1 Problems can arise from some means of representing dates in computer equipment and products and from date-logic embedded in purchased goods or services, as the year 2000 approaches and during and after that year. As a result, equipment or products, including embedded control logic, may fail completely, malfunction or cause data to be corrupted.

1.2 To avoid such problems, organizations must check, and modify if necessary, internally produced equipment and products and similarly check externally supplied equipment and products with their suppliers. The purpose of this document is to allow such checks to be made on a basis of common understanding.

1.3 Where checks are made with external suppliers, care should be taken to distinguish between claims of conformity and the ability to demonstrate conformity.

2 Amplification of the definition

2.1 PD2000-1 (all editions) is solely concerned with the performance and functionality of a single version, release or system. It does not address differences in performance or functionality between different versions, releases or systems.

2.2 Variations in performance immeasurably small in the context of use do not make a version, release or system non-conformant.

3 Amplification of the Rules

3.1 Rule 1

3.1.1 This rule is sometimes known as general integrity.

3.1.2 If this requirement is satisfied, roll-over between all significant time demarcations (e.g. days, months, years, centuries) will be performed correctly.

3.1.3 Current date means today's date as known to the equipment or product, i.e. the actual date of operation [NOTE - this refers to normal operation and does not prevent testing.]

3.2 Rule 2

3.2.1 This rule is sometimes known as date integrity.

3.2.2 This rule means that all equipment and products must calculate, manipulate and represent dates correctly for the purposes for which they were intended.

3.2.3 The meaning of functionality includes both processes and the results of those processes.

3.2.4 If desired, a reference point for date values and calculations may be added by organizations; e.g. as defined by the Gregorian calendar.
3.2.5 No equipment or product shall use particular date values for special meanings; e.g. "99" to signify "no end value" or "end of file" or "00" to mean "not applicable" or "beginning of file" unless the values in question lie outside its possible date range.

3.3 Rule 3

3.3.1 This rule is sometimes known as explicit/implicit century.
3.3.2 It covers two general approaches:
(a) explicit representation of the year in dates: e.g. by using four digits or by including a century indicator. In this case, a reference may be inserted (e.g. 4-digit years as allowed by ISO 8601:1988) and it may be necessary to allow for exceptions where domain-specific standards (e.g. standards relating to Electronic Data Interchange, Automatic Teller Machines or Bankers Automated Clearing Services) should have precedence.
(b) the use of inferencing rules: e.g. two-digit years with a value greater than 50 imply 19xx, those with a value equal to or less than 50 imply 20xx. Rules for century inferencing as a whole must apply to all contexts in which the date is used, although different inferencing rules may apply to different date sets. Where any date element is represented without a century, the correct century shall be unambiguous for all manipulations involving that element.

3.4 Rule 4

3.4.1 A leap year is defined in ISO 8601:1988 (amended in 1991) as follows:
"year, leap: In the Gregorian calendar, a year which has 366 days. A leap year is a year whose number is divisible by four an integral number of times, except that if it is a centennial year it shall be divisible by four hundred an integral number of times."
3.4.2 Thus, for example, 2000 is a leap year but 1900 is not.

4 General Notes

4.1 For Rules 1 and 2 in particular, it is recommended that the allowable ranges for values of current date and dates to be manipulated be documented, recognizing that all systems have some limitation on the valid date ranges. The ranges may relate to one or more of the feasible life-spans of equipment or products or the span of dates required to be represented by the organization's business processes.
4.2 Tests for specifically critical dates may also be added (e.g. for leap years, end of year, etc.). Organizations may wish to append additional material in support of local requirements.
4.3 Where the term "century" is used, clear distinction should be made between the "value" denoting the century (e.g. 20th) and its representation in dates (e.g. 19xx); similarly, 21st and 20xx.

Appendix 2

Appendix 2:
Year 2000 Compliance Testing Guidelines

1. Compliance Testing For Operating Systems
BSI Compliance Criteria: Test For Impact Analysis

Rule 1 General Integrity
The system date can be set to the high-risk dates: 31-12-1999, 01-01-2000, 29-02-2000. The system will reinitialise from cold start on the high-risk dates: 31-12-1999, 01-01-2000, 29-02-2000. The system date rolls over correctly on the high-risk dates: 31-12-1998 to 01-01-1999, 31-12-1999 to 01-01-2000, 28-02-2000 to 29-02-2000, 29-02-2000 to 01-03-2000. The system date rolls over correctly in both powered-up and powered-down states.

Rule 2 Date Integrity
The date-sensitive functions for system dates behave correctly in 19xx and 20xx. Date-sensitive refers to functions whose behaviour can start or stop on a specified date, on a specified day of the week, or after a specified elapsed time. Functions such as job scheduling, accounting, administration functions, any interactive command with dates in parameters or switches (especially disk and tape commands and utilities) function correctly. Setting or obtaining the system date through a system call, and reporting system data with dates in it, gives the correct result. What is highest possible value that can represent the system date? The system date appears correctly in time-stamps for queue entries, volume directories, inter-process communication, and off-host communication on the high-risk dates: 01-01-1999, 31-12-1999, 01-01-2000, 28-02-2000, 29-02-2000, 01-03-2000.

Rule 3 Explicit Century
The century be explicitly entered or displayed in date-sensitive functions. If there are functions or system calls which cannot permit an explicit century, is the format governed by an industry standard or customer requirement?

Rule 3 Implicit Century
Could the century in any date value in any date-sensitive function be misinterpreted for dates between 01-01-1985 and 01-12-2050? What algorithm is being used to map implicit centuries?

Rule 4 Leap Year
The system correctly rolls over from 28-02-2000 to 29-02-2000, and from 28-02-1900 to 01-03-2000.

2. Compliance Testing For A Database Management System (DBMS)Compliance Criteria Test For Impact Analysis

Rule 1 General Integrity
Does the language provide a function to obtain the system date on the host or through a time service? Does this function return the correct value for the system date for the high-risk dates: 31-12-1999, 01-01-2000, 29-02-2000. This function returns the correct value for the system date after the system date rolls over on the high-risk dates: 31-12-1998 to 01-01-1999, 31-12-1999 to 01-01-2000, 28-02-2000 to 29-02-2000, 29-02-2000 to 01-03-2000.

Rule 2 Date Integrity
The language supports a data type for date values in the range 01-01-1900 to 31-12-2050. The date arithmetic correctly calculate differences between dates, addition of dates and duration's, and computes the day of the week. The language routines correctly convert between date representations (YMD to Julian to base-and-offset internal). The language correctly compare dates. If a key index includes a date field, is the correct sequence produced across dates in 19xx and 20xx? The DBMS retrieves dates accurately for values in the range 01-01-1900 to 31-12-2050.

Rule 3 Explicit Century
The date data type permits setting explicit values for century. The retrieval functions permit formatting dates with explicit century. The DBMS retrieves date values accurately for values in the range 01-01-1900 to 31-12-2050.
Rule 3 Implicit Century
Does date data type provide for data types without explicit century? If the value for the century is not explicitly set, what value is assumed in setting the date field to a value, date comparisons, date arithmetic, etc.? What algorithm is used to map implicit centuries?

Rule 4 Leap Year
The language routines treat 2000 as a leap year and 1900 as a non-leap year.

2. Testing Compliance Of A Custom Application
Compliance Criteria: Test For Impact Analysis

Rule 1 General Integrity
Does the language provide a function to obtain the system date on the host or through a time service? Does this function return the correct value for system date for the high-risk dates: 31-12-1999, 01-01-2000, 29-02-2000. This function returns the correct value for system date after the system date rolls over on the high-risk dates: 31-12-1998 to 01-01-1999, 31-12-1999 to 01-01-2000, 28-02-2000 to 29-02-2000, 29-02-2000 to 01-03-2000. Does the application code ignore values for explicit century in the system date at any point in the program logic? Are there any third-party products embedded in this application? Are all these products century-compliant?

Rule 2 Date Integrity
The programming language supports a data type for date values in the range 01-01-1900 to 31-12-2050. The date arithmetic correctly calculate duration's (differences) between dates, addition of dates and duration's, compute date of week. If the application compares dates in any of its branching logic or calculation of Boolean values, do all these comparisons produce correct results for all combinations of values with the expected ranges for dates? Does the application convert date values from one representation to another (for example, YMD to Julian to base-and-offset internal)? Does software correctly convert between date representations according to the Gregorian calendar? If the application includes searching, sorting, merging, or indexing on internal tables, linked lists, or other data structures based on date variables, do these operations perform correctly for all possible values for date in the key variables? If a key index includes a date field is the correct sequence produced across dates in 19xx and 20xx? Does the application use language features which map a data address to more than one variable (such as REDEFINE's in COBOL)? In all aliases for the same data space, does any variable ignore or truncate a value for explicit century in the

date value? Is the truncated value for date eventually used in a manipulation which assumes that all values for date share the same century? Does the application represent date in any variable as an offset from a base date/time? What is the maximum value for date for this representation? What is the minimum value for date for this representation (usually the base date)? Does the expected range of values for each variable using this date representation fall within these extremes? If the application assigns date values from one variable to another, is the century portion of the value truncated during the assignment? Is the value in the target variable eventually used in a date manipulation which requires explicit century for correct results? Does the application use sort/merge utilities to order file contents on date fields or use indexed file structures keyed on date fields? Is this order correct for all values of date in the range 01-01-1900 to 31-12-2050? If constants for date values (including day, month, or year) are used in any manipulation, is the date constant intrinsic to the functional requirements or a special value used in a "date" data type for convenience? The application stores and retrieves dates accurately for values in the range 01-01-1900 to 31-12-2050. Does the application rely on a primary indices on a structured database for search, insert, update, or delete in which any key contains a date field? Will the index order be correct for all values for date in the range 01-01-1900 to 31-12-2050? Are all date variables initialised to some convention for the null value?

If the application uses constant values for dates or portions of dates (i.e., day, month, or year), then for any constant which is a full date value or value for the year, is the century not explicit in the value? Do all manipulations using each constant value directly or indirectly (that is, carried via variables to other operations in the program logic), produce the correct results for all possible values for such date variables? Does the application support a user interface containing date fields without explicit century? Is the century in each unambiguous to a user for all possible values for date in each such field? Does the application use any application program interface (API), such as in-line SQL, which passes date variables? If so, for any date value supplied across this interface, does the receiving software provide a default or derived value of the century? Are the rules for derivation on both sides of the interface consistent with each other for possible values for date in the respective fields? Do all representations of date both internal to the application and in all interfaces satisfy the criteria for century compliance?

Rule 3 Explicit Century

If the application uses a language, toolkit, and/or application generator which permits explicit century in the date data types, are the values for the century in variables of these types supplied from external input or derived within the software logic? Does the application use a DBMS or other software product to store and retrieve date variables? If so, can these products support explicit values for century in any date variable stored and retrieved? Does the application have external interfaces (I/O, APIs, library routines) which contains a date variable with explicit century? Does the software truncate, or write over the century value in any such variable as it flows through the program logic to any external interfaces? In any such flow, could any logic alter the value for century in any manner inconsistent with generalised manipulations based on the Gregorian calendar?

Do all representations of date with explicit century both internal to the application and in all interfaces satisfy the criteria for century compliance?

Rule 3 Implicit Century

Does the application use a language, toolkit, and/or application generator (including GUI

builders) which permits date representation without an explicit century in the date data types? If so, is the century derived for any manipulations or for passing a date value across any interface or for permanent storage? If so, is value for the century correct for all values possible values of date each such variable can hold?

Rule 4 Leap Year

If the application makes any leap-year calculations, do these calculations treat 2000 as a leap year and 1900 as a non-leap year?

NB. The material in this section - "Year 2000 Compliance Testing Guidelines" may be freely copied provided that the source is acknowledged (BSI-DISC), and it is reproduced in full.

The Futures and Options Association
One America Square
17 Crosswall
London EC3N 2PP

Tel: 0171 426 7250
Fax: 0171 426 7251
www.foa.co.uk
e-mail: info@foa.co.uk