Year 2000 Business Continuity Planning: Guidelines for Financial Institutions

Introduction

The purpose of this paper is to help financial institutions, in particular their senior management, address business continuity planning in the context of the transition to the Year 2000. This issue should be at the top of the senior business decision-maker's agenda during 1999. It is important that firms understand the need to develop specific Year 2000 contingency plans as soon as possible and the reason why it is not possible to rely exclusively on existing plans for this purpose.

Year 2000 continuity planning is about ensuring the continuous and efficient functioning of business activities during the transition to the new millennium, not about providing backup for computer systems. It should therefore be approached in a market and business context, not as a technical project, and should be treated as a top business priority by the boards and senior management of financial institutions. The focus should be on core business activities, that is, those on which the survival of the business depends.

There are various critical stages in the transition to the Year 2000. These relate in the first instance to the different dates on which information systems might face date-related difficulties in the course of 1999 and 2000. They also relate to different deadlines which the firm might face for internal as well as external testing and for reacting to any unexpected problems that might occur at such times. Problems with the various external dependencies of the firm, including third-party suppliers, market infrastructures, counterparties, clients and public utilities, might occur at different times during the transition. Finally, the firm will have to carefully approach the century date change in its computer applications, for instance by freezing system changes at the end of 1999 and gradually introducing new applications during the course of 2000.

Planning for the various possible Year 2000 eventualities and developing procedures for dealing with any contingencies will take time. This is why financial firms should start their Year 2000 continuity planning as soon as possible. To delay starting is to risk business interruption and may diminish the credibility of the business in the eyes of customers, counterparties and other third parties (including financial market regulators).

Increasingly, as 1999 progresses, institutions should ensure that they are ready to provide factual information about the state and nature of their Year 2000 preparedness and continuity planning. Requests for information could originate, internally, from the different business units and, externally, from those parties to which the firm’s business continuity is important. It will therefore be important for the firm to develop appropriate communication strategies, both internal and external.

Part 1 of this paper explains in more detail why all financial institutions must develop Year 2000 business continuity plans and why work should start as soon as possible. It also describes the general approaches that should be adopted in developing and implementing plans, and the responsibilities of senior management.

Part 2 provides more specific guidance on the main features of a business continuity project. Good practice on this topic will evolve as 1999 progresses and firms are actively encouraged to study how they can include existing and evolving best practices in their own approach. In this respect, cooperation with other financial market participants and with regulators will be useful. The Joint Year 2000 Council or its parent committees may publish further guidance if this seems appropriate.

1. The general approach to Year 2000 business continuity planning

In order to develop an effective and workable approach to Year 2000 business continuity planning, senior management must understand the challenges involved in ensuring business continuity during the transition to 2000 and the need to start work in this respect as soon as possible. This part of the paper addresses these issues and explains the general approach to Year 2000 contingency planning.

1.1 The importance of Year 2000 business continuity planning

Financial institutions throughout the world are actively addressing the Year 2000 problem. The focus has been on *awareness, assessment, remediation, testing and implementation* with a view to achieving business continuity so far as mission critical business activities are concerned. Many observers believe that financial sectors in many countries will achieve a high state of Year 2000 preparedness.

However, because of the nature of the Year 2000 problem, no institution will be able to assume that it has removed all threats to business continuity. Even if an institution believes that it has reasonable grounds for a high degree of confidence in the effectiveness of its own Year 2000 programme, and in the Year 2000 programmes of others, it will remain possible for problems to occur in different areas. These include: the firm's own systems; the systems of an entity to which it has outsourced some of its operations; the systems of a financial infrastructure provider such as a clearing and settlement system or message carrier; and the systems of a major business dependency such as a correspondent, trading counterparty or large client. Moreover, the firm itself and all the relevant external parties are vulnerable to possible disruptions at public utilities such as telecommunications, electricity, water, sewage or transport operators. The nature and scale of Year 2000 challenges and programmes is such that there can be no certainty in advance that assessment, remediation, testing and implementation activity both within and outside the firm has been fully effective.[1]

Although most problems are likely to be caused by operational failures, they will directly threaten business continuity. Thorough business continuity planning is therefore a matter of simple prudence and it must be an integral part of every institution's Year 2000 strategy.

Most institutions have contingency plans, for example for computer breakdowns or fire or other physical disasters. These may be a valuable starting-point for Year 2000 continuity planning. However, conventional contingency plans will not be adequate to deal with Year 2000 problems. For example, backup computer systems are likely to replicate faults in the main hardware and software systems and may not be available if they are maintained at sites operated by a third party that could face Year 2000 difficulties.[2] Difficulties could also be encountered in different business areas at the same time, and initially small and localised problems could combine to create larger disturbances. Problems, one's own or those of others, might well be more difficult to diagnose and may take longer to put right. Particular solutions may not work if adopted and used simultaneously by a large number of institutions (e.g. simultaneous mass faxing if there is a problem with voice telephony). Most importantly, the behaviour and perception of external parties, including customers, trading counterparties and correspondents, may change individually or collectively (on the basis, for instance, of rumour or speculation).

A further important factor is that although 1 January 2000 (like other sensitive dates in this context) is fixed, information for example about an institution, industry sector or region's preparedness is likely

---

1 See the Joint Year 2000 Council's paper "Scope and Impact of the Year 2000 problem".

2 The capacity of backup sites provided by third parties might also prove insufficient if a large number of customers request support at the same time.

to emerge throughout the period before, during and after 1 January 2000. This will require the risks to be reassessed on an ongoing basis and the plans to be adapted accordingly.

1.2 The need to start Year 2000 continuity planning as soon as possible

Given all that is involved, the start of continuity planning cannot be left until the end of Year 2000 preparatory work. At the same time, continuity planning must not be done in a way which prejudices the successful and timely completion of the other key elements of a Year 2000 programme.

For the reasons given above, institutions must treat the Year 2000 as a potential problem without precedent. The issues that need to be addressed are many and wide-ranging. Institutions must carry out a specific Year 2000 risk assessment and will need to draw up new plans to address the risks they identify. They should, as far as possible, test those plans in advance. Developing and implementing a credible plan will therefore require significant resources and effective organisation. No doubt this will also take time, and work should therefore be started as soon as possible. To delay starting is to risk not having an adequate plan in time.

All institutions should aim to have a business continuity project in place as early as possible, preferably by the end of the first quarter of 1999. The project should include a timetable which provides for a business continuity plan to be completed by September 1999. Throughout the process, institutions need to ensure that work is prioritised so that there is an appropriate focus both in terms of what is most critical to the business and in terms of timing (e.g. between pre and post-1 January 2000 issues).

1.3 The general approach to Year 2000 continuity planning

For all institutions, addressing such an unprecedented problem will be very challenging. Many will have their own approach to contingency planning, which may well provide a sound methodology, and there are advantages in using familiar methods. However, what is essential is the full and active involvement of senior management and all business units in the process.

Most institutions will look in the first instance to their own resources, for example within their Year 2000 programme[3] or their risk management teams, supported by internal audit, to address Year 2000 continuity planning. However, given the unprecedented characteristics of the problem, every institution should make itself open to outside information, advice and support in order to receive the full benefit of professional expertise and practical experience as well as, if necessary, the requisite resources.

Particular caution should be exercised with regard to relying on resources employed in the Year 2000 programme for the development and implementation of a Year 2000 continuity project. One reason is that the Year 2000 programme will involve rigorous and continuous testing and careful implementation of remediated systems throughout 1999. Technical experts involved in the Year 2000 programme will also need to remain available during all the important phases in the transition to 2000 in order to deal with any unexpected difficulties that might arise. Part 2 of this paper contains more specific guidelines on the development and implementation of the business continuity project. These are based on a number of guides to Year 2000 contingency planning that are now available from, or are being prepared by, regulatory organisations or trade bodies (see Annex). Specialist consultancy and accounting firms have also developed guidelines for proper Year 2000 contingency planning. Moreover, some individual firms which have recognised at an early stage that the Year 2000 should not be treated as a competitive issue have been willing to share information on their own practice and

[3] To avoid confusion in this document, the main Year 2000 project aimed at remediating and testing the systems is called the Year 2000 programme, while the project aimed at providing business continuity is called the Year 2000 business continuity project.

experience. Finally, in some cases national Year 2000 coordinators are providing guidance to companies.

Most of these documents clearly state that Year 2000 business continuity is not a technical issue and should receive the attention of senior managers. Their involvement is required to ensure appropriate accountability and commitment, proper organisation and extensive coverage. It will be their responsibility to take decisions that relate to the core business strategies.

With respect to *accountability*, senior management should sponsor the business continuity project and provide adequate resources to put in place an effective business continuity plan in good time. They must ensure the adequate participation of all major business units. They will have to approve the risk assumptions and analysis and endorse the plans for risk mitigation and management.

As with the Year 2000 readiness programmes, the development of the business continuity project will require proper *organisation.* A timetable, with milestones, will need to be drawn up and adhered to, which will necessitate conferring the proper authority on the project group. Coordination with the main Year 2000 readiness programme as well as with the major business units will be a major challenge.

A proper organisation team(zero day management) has to be put in place for the Year 2000 transition period. This team should be responsible for collecting and disseminating information inside and outside the institutions and should have decision-making capabilities.

Ensuring *extensive coverage* of the Year 2000 continuity project will require executive attention. Adequate assumptions, scenarios and plans will need to be developed to cover the risks to which the firm is exposed before, during and after 1 January 2000, including operational, financial and reputational risks. This should take into account the vulnerabilities to the firm's own systems as well as to those of relevant external parties.

2. Guidelines on business continuity projects

This part of the paper provides more specific guidance on the development and implementation of a business continuity project. Institutions should consider it in the context of their own particular circumstances, organisation and working methods.

2.1 Establish high-level commitment to a business continuity project

The purpose of a business continuity project is to maximise the ability of the business to maintain a minimum level of outputs and services and the confidence of customers, counterparties and other key third parties in adverse circumstances. It should also help to identify alternatives to normal business processes and to prepare for a possible crisis. In the event of emergency measures being invoked, the business continuity project should facilitate the rapid resumption of normal service.

The establishment of a business continuity project may be a matter of business survival. It requires the rigorous identification of the risks to what is critical for adequate business continuity as well as the development and implementation of strategies to reduce those risks (*risk prevention*) or to mitigate the impact of any problems that occur in practice (*risk mitigation*).

As indicated in Part 1, the exposure to risk during the transition to the Year 2000 is likely to be greater than normal. Accordingly, it is prudent for institutions to assume that problems of some kind will occur and that those problems may well be unusual. Nevertheless, institutions should take existing business continuity plans into account and retain what remains appropriate in a Year 2000 context.

An effective project will be a complex, business-critical and resource-intensive task. It is essential that boards and senior managements take direct responsibility for the establishment of a project with the objective of achieving an agreed business continuity plan and for the allocation of sufficient resources. Their input is essential, in particular with respect to the formulation of the strategic business priorities

that will need to be reflected in the plan. They must also lend the project the necessary support to ensure that its importance and priority are recognised by the business as a whole. Finally, they should monitor its execution, on the basis of regular reporting.

The business continuity project should be given an identified project manager and a project team of a sufficient size and quality to ensure its timely completion. All relevant business areas also need to be involved in the project in order to ensure their commitment and contribution of expertise and knowledge. This is likely to encompass the major business units, disaster recovery specialists, systems and operations units, and legal counsel.

The relationship of the project to the Year 2000 programme should be made clear. It should ensure the effective exchange of relevant information and coordination between the two projects. As explained in Part 1, the objectives and scope of the two projects are different and it is therefore advisable to establish them separately, with different project managers and staff. The business continuity project is likely to be most effective if it is sponsored by senior management.

2.2 Establish a project plan and timelines

A first task of the project team should be to establish a project plan which identifies the scope of the project, allocates responsibilities for each project task and lays down timelines for each stream of work. This plan should be approved by the project team as a whole and endorsed by senior management. The timelines should be sufficiently detailed, with milestones, to enable progress on the plan to be regularly reviewed by both the team and senior management.

The scope of the project plan, and the timelines, should be kept under review and adjusted as necessary, in the light of experience or new information. Any threats to the achievement in good time of an effective business continuity strategy should be identified and addressed as and when they arise.

2.3 Identify business critical systems and processes

An essential objective of the business continuity project would be to identify what is critical to the continuity of business. This includes the key systems and processes which support the critical services and the internal and external dependencies which are crucial to the business. Much of this information should have been obtained in the context of the Year 2000 programme. However, the business continuity project should itself ensure that the risks to business continuity are addressed comprehensively. The project team should therefore review the analysis made in the main programme.

The business continuity project and the Year 2000 programme should generally agree on what is considered to be business-critical so that the business as a whole operates on the basis of a consistent, agreed analysis. Any inconsistencies or disagreements should be resolved at senior level.

2.4 Establish a risk identification and assessment methodology

To meet the primary purpose of an effective business continuity project it is essential to put in place a methodology for identifying the risks to business continuity and assessing their potential impact. That methodology must then be applied across the business as a whole. The methodology should be one which is practical, straightforward and readily understood by all those in the business who need to use it. It should also ensure comprehensive risk identification and assessment and be cost-effective.

The identification of the business's key processes, systems and dependencies (both internal and external) should provide the starting-point for identifying the risks. The business continuity project should consider the risks attaching to the Year 2000 programme itself, such as the failure to complete the programme in time and inadequacies or errors in one of the programme elements (e.g. inventory or testing). In addition, the business continuity project must consider the risks arising from the overall environment in which the business operates. These risks are likely to fall into one of three broad categories: operational risks, credit and liquidity risks and reputational risks.

Operational risks could arise from failures in internal systems, problems with facilities such as lifts, air-conditioning, heating or backup power supplies, and disruptions in the services provided by utilities such as water, electricity and telecommunications. They could also result from disturbances in financial market infrastructure elements such as payment and settlement systems, exchanges, market information providers or message carriers. Special attention should also be paid to the fact that frauds may be attempted when operational difficulties are experienced and normal business functioning (and security) is impaired.

Credit and liquidity risks are the typical financial risks to which financial institutions are exposed. Credit risk involves the possible financial loss as a result, for instance, of a counterparty default or the depreciation in value of the assets held by the institution. Liquidity risk arises when financial institutions face unexpected cash-flow positions and either have to fund cash-flow shortfalls at short notice and unfavourable terms or invest surplus funds under unattractive conditions. In the context of the Year 2000, such risks can arise in different ways when financial institutions cannot carry out their business as usual. Particular concerns relate to the ability of firms to trade and settle under normal conditions and markets to function smoothly and with the needed liquidity when uncertainty increases.

Reputational risk can occur when a financial institution is seen to be poorly prepared to deal with operational or financial difficulties and when incidents occur that impair the institution's ability to operate normally and efficiently. This can result in the institution being negatively perceived by customers, counterparties or market participants. Given the degree of uncertainty about Year 2000 preparations, as well as the multiple interdependencies between financial market participants and their joint dependence on third-party service providers, it is likely that financial firms will face Year 2000 disruptions. There is therefore strong potential for the reputation of financial firms to be negatively affected by Year 2000 difficulties in the financial system (whether real or perceived). [4]

Institutions need to be imaginative in identifying the possible risks. All parts of the business need to be involved to ensure that the process of risk identification results in a comprehensive list of perceived risks to business continuity.

For each of the types of risk identified, a proper assessment must be made of the probability of the risk occurring and the impact on the business if it does occur. The impact assessment should make explicit assumptions about the expected duration of a problem, for example, one hour, one day or one week. The purpose of this assessment is to enable the business to identify those risks which are most likely to occur and whose impact could be significant. It would also allow the identification of those risks whose impact would be very high, even if the probability of occurrence is low. A simple methodology can be used, for instance classifying probability and impact (separately) on a high/medium/low basis.

It is essential that the analysis involve those in the business who are best placed to make the assessment by virtue of their knowledge, experience or expertise. In particular, business managers, who are in the best position to identify, assess and address risks to business viability, should be directly involved.

2.5 Develop risk prevention and mitigation measures

After carrying out making the risk assessment, judgements should be made as to which risks present sufficient threats to the business to require the development of strategies and actions to prevent them arising or to mitigate their impact if they do arise. These judgements should be the basis for prioritising work in the project.

There may be various options for risk prevention and mitigation, including:

---

[4] As indicated in the Council's policy paper on disclosure and information sharing (January 1999) this is one reason for financial firms to take voluntary action to publicly disclose information about their readiness programmes and contingency plans.

– continuous review of results of tests on own systems (including those with embedded chips) and those of external parties;

– rigorous prior assessment and continuous review of readiness and contingency plans of key market infrastructure providers, customers, counterparties, public utilities and government agencies;

– reducing legal exposure, for instance by renegotiating contracts or revising documentation;

– developing an effective disclosure and communications strategy;

– working with other market participants, industry associations and market infrastructure providers to review best practices and, where appropriate, develop joint initiatives, for instance with respect to market practices;

– enhancing liquidity and access to liquidity;

– developing alternatives to normal business processes, for instance manual procedures or access to alternative types of trading procedure;

– disaster recovery plans in the event of problems with availability of buildings, staff, etc.

Options should be chosen according to the likely seriousness of the expected disturbances and on the basis of their feasibility and the general business priorities. The overall objective should be to prepare to deal with contingencies without creating a false sense of security or an unnecessary degree of anxiety. Particular attention should be paid to internal and external communication strategies.

2.6 Zero day information management, communications and decision-taking

A business must be organised and prepared in the run-up to, on and after 1 January 2000, the so-called "zero day", to acquire and use information about itself, about third parties and about the general environment, including the infrastructure that may be relevant to business continuity. Information must be available at all times to allow rapid decisions to be made in response to developments in order to sustain business continuity. Finally, a firm must be able to communicate about its own status to regulators, business partners, customers and the media.

For this purpose, the business should, well in advance, identify the information likely to be required by itself and by others, the sources of that information, the means of obtaining it and the persons to whom the information is to be made available. This is likely to have implications for communications arrangements, internal and external, and for the availability of personnel.

The business should also, well in advance, determine the management arrangements for decision-making and the staff who will need to be involved in those arrangements. The facilities and support necessary to ensure that arrangements work efficiently should also be identified.

A business may consider it necessary to establish one or more communications or command centres to facilitate the dissemination of information and the monitoring of developments. Appropriate channels for information flows should enhance internal consultation and decision-making. To be effective, all these arrangements should be tested in advance.

2.7 Process discipline

All risk prevention and mitigation plans should be developed in accordance with strict process disciplines. This would require: precise documentation of each risk and of the related prevention or mitigation strategy; allocation of responsibility to an individual to develop and implement the strategy; and approval at the appropriate management level of the strategy and implementation plans.

It is also essential that, so far as practicable, each plan be tested to identify gaps or problems and to verify its credibility. Where necessary, the plan should be modified in the light of the tests. Those who will have to implement the plan must receive appropriate guidance and training.

Throughout the period before, during and after 1 January 2000, the business must be constantly on the alert for new developments or information that may change the risk identification or assessment or the assumptions made. The business continuity plan should be adjusted as necessary. In particular, in the context of business continuity planning as in the main remediation programme, institutions must be alert to the implications of and risks attaching to changes made by the business to IT systems or programmes, or to business processes, outside Year 2000 projects. Institutions should seek to minimise such changes, particularly as 1 January 2000 approaches.[5]

[5] Refer to Council's press statement and quote private and public sector recommendation to change management …

Annex

Source	Date	Title	Available from
French financial sector (supervisory authorities and market participants)	February 1999	Addendum to the White Book on the Year 2000 changeover - Business continuity after 2000	www.an2000.gouv.fr www.banque-france.fr
Global 2000 Co-ordinating Group	January 1999	Year 2000 Business Risk Management	www.global2k.com
Hong Kong Monetary Authority	December 1998	Guidance Note on Year 2000 Contingency Planning by Authorised Institutions	www.info.gov.hk/banking/guideline/981214.htm
Bank of Japan	November 1998	Guidance on Year 2000 Contingency Planning	www.boj.or.jp
US General Accounting Office (GAO)	August 1998	Year 2000 Computing Crisis: Business Continuity and Contingency Planning	www.gao.gov/special.pubs/bcpguide.pdf
British Bankers' Association (BBA)	October 1998	Year 2000 Contingency Planning Guide	www.bankfacts.org.uk
Federal Financial Institutions Examination Council (FFIEC)	13 May 1998	Guidance concerning Contingency Planning in connection with Year 2000 Readiness	www.ffiec.gov/y2k