YEAR 2000 BULLETIN

Hong Kong Monetary Authority

December 1998

Introduction

This Year 2000 Bulletin is the third of a series providing a channel for the Hong Kong Monetary Authority ("HKMA") to promote awareness and sharing of sound practices in addressing the Year 2000 issue within the banking industry in Hong Kong.

Certain articles in this issue of the Bulletin are contributed by market practitioners. The guidance or advice contained in these articles is largely advisory in nature and does not represent requirements of the HKMA. The HKMA would like to thank Mr Tim Janes of PricewaterhouseCoopers and the Hong Kong Interbank Clearing Limited for their contribution.

In this issue...

Recent Developments & Supervisory Initiatives on the Year 2000 Problem

We are now less than 370 days from the Year 2000, which makes it more important than ever for authorised institutions ("AIs") in Hong Kong to ensure that they take adequate steps to address the millennium transition. As institutions are aware, the HKMA has established 31 December 1998 as the deadline by which all AIs are expected to achieve Year 2000 compliance. Institutions should therefore be close to completing the testing phase of their Year 2000 programmes. This will leave them time to conduct testing with external parties in 1999. In addition, institutions should have commenced the implementation of a counterparty assessment framework and contingency planning for the Year 2000. The HKMA has issued a guidance note on counterparty assessment and has required AIs to largely complete the process by end-March 1999. The HKMA has also issued a guidance note on contingency planning to recommend all AIs to largely complete the development of their Year 2000 contingency plans by end-March 1999 and the testing of their plans by end-June 1999. These two guidance notes are available on the HKMA's web-site.

Preparedness of the banking sector

The HKMA has reviewed the third formal statements submitted by the chief executives ("CEs") of AIs. The results as at end-September 1998 indicate that:

- The percentages of AIs expecting to achieve compliance by end-1998 for their critical and non-critical systems are 94% and 88% respectively;
- The overall percentages of completion for critical and non-critical systems are 82% and 77% respectively;
- On average, AIs have spent 64% and 56% of their budgets on critical and non-critical systems respectively;

Results of Formal Statements

	Reported positions as at end-	
	September 1998	July 1998
Percentage of AIs expecting to achieve compliance by 31 December 1998 for:		
- critical systems	94%	95%
- non-critical systems	88%	86%
Percentage of completion for critical systems:		
- assessment phase	98.42%	97.70%
- modification phase	90.03%	79.56%
- testing phase	71.28%	54.80%
Percentage of completion for non-critical systems:		
- assessment phase	96.88%	95.30%
- modification phase	82.96%	70.55%
- testing phase	65.77%	49.52%
Overall percentage of completion on:		
- critical systems	82.24%	72.00%
- non-critical systems	77.01%	64.76%
Overall percentage of budget spent on:		
- critical systems	64.28%	55.15%
- non-critical systems	55.88%	44.03%
Percentage of CEs satisfied with overall progress made to date and sufficient resources devoted:	95.14%	93.64%
Percentage of AIs which have not experienced significant delays and problems in the project:	93.92%	92.42%
Percentage of CEs satisfied with progress made to date to address counterparty risks:	87.23%	83.03%
Percentage of CEs satisfied that there are adequate contingency plans in place:	74.16%	73.03%

- 95% of CEs are satisfied with the overall progress and resources devoted to the projects; and
- On average, AIs have completed 98% of the assessment phase, 90% of the modification phase and 71% of the testing phase with respect to their critical systems.

The results demonstrate that the banking industry continues to make good progress in achieving Year 2000 compliance. In particular, notable advancement has been made in the modification and testing of critical systems. However, the results also indicate that there are several AIs which do not expect to achieve compliance for all their critical systems by 31 December 1998. Most of the AIs have attributed the delay to the time required to replace a few particular critical systems. A few AIs also reported that priority has been given to the euro.

The HKMA is most concerned about those institutions which are unlikely to achieve critical system compliance by the end-1998 deadline. We have issued formal notices to the CEs of these institutions to require them to take every effort to achieve critical system compliance by end-March 1999. Further, the HKMA has made clear to these institutions that if it does not appear that every effort is being made to achieve compliance, the HKMA will consider use of its statutory powers under the Banking Ordinance to enforce compliance with the deadline.

Definition of Critical Systems

The HKMA has come across cases whereby different institutions have adopted different definitions in respect of their critical and non-critical systems. To avoid confusion and to provide a reference point, it should be reiterated that the HKMA has adopted the following definition for critical systems:

> "Any centralised or decentralised computer hardware, software, networks, or equipment with embedded computer chips and logic, e.g. security systems, elevators, vaults, of an AI is a critical system if at least one of the principal businesses of the institution will be disrupted or considerably impaired as a direct or indirect consequence of abnormal performance or functionality of the system."

The HKMA expects AIs to adopt the same or a similar definition. Depending on the principal businesses and core functions of AIs, critical systems usually cover payments, accounting, treasury, risk management, front office, communications and operating systems directly supporting essential banking services.

Contingency Planning

The HKMA is concerned that disruptions in bank operations as a result of the failure of systems to correctly process transactions involving the Year 2000 could have a significant adverse impact on the stability of the banking sector. Apart from requiring AIs to formulate contingency plans, the HKMA is also in the process of preparing its own contingency plan for the banking sector as a whole. The objectives of the contingency plan are:

- To cater for potential systemic problems in relation to the banking sector arising from the Year 2000 problem; and
- To ensure consistence of the HKMA's contingency plan with that being formulated by the Steering Committee on Year 2000 Compliance in the Financial Services Sector to handle potential systemic problems in the financial sector in Hong Kong.

Steering Committee on Year 2000 Compliance in the Financial Services Sector

In October this year, the Steering Committee issued a report which summarises the position of the Year 2000 external testing activities in the financial services sector in Hong Kong. The information contained in the report provides a good understanding of what the financial services sector in Hong Kong has done or is planning to do to enhance its Year 2000 readiness. This report has received very good response from the international financial community. The Joint Year 2000 Council is considering adopting the framework of the report to update a survey on the Year 2000 preparedness of financial systems around the world. The report can be downloaded from http://www.info.gov.hk/fsb/year2000/content.htm.

Testing of Interbank Payment Systems

The Year 2000 external end-to-end testing of the interbank payment systems organised by the Hong Kong Interbank Clearing Limited ("HKICL") was completed in early November this year as scheduled. No abnormalities relating to the Year 2000 problem were reported to the HKICL. Two additional rounds of end-to-end testing will be conducted in 1999 to provide opportunities for banks to further validate the compliance of their interfaces with the interbank payment systems before the millennium. (Please see separate article prepared by HKICL in this issue.)

Disclosure of Year 2000 Progress by AIs

To facilitate wider access to AIs' disclosure of Year 2000 progress through the Internet, the HKMA has established a hyperlink from its homepage to those of the AIs which have forwarded their web-site addresses to the HKMA. To date, we have established hyperlinks to over 30 AIs or their head offices through the Internet.

External Testing of Interbank Payment Systems

The Year 2000 external end-to-end tests of the interbank payment systems organized by the Hong Kong Interbank Clearing Limited ("HKICL") have been completed as scheduled. Throughout the tests, no Year 2000 exceptions were identified. HKICL will organise additional testing sessions in 1999 to provide opportunities for banks to further validate the compliance of their interfaces with the interbank payment systems before the millennium date change. HKICL is also working on its Year 2000 contingency plan.

Rectification of Internal Systems

HKICL completed the internal end-to-end testing of its computer systems in June 1998 and confirmed that they are Year 2000 compliant. Year 2000 compliant certificates have been solicited from vendors of the office equipment and environmental facilities i.e. backup generator, uninterruptible power supply, air-conditioning etc. and testing is being performed to the maximum extent allowed.

External Interface

The end-to-end external testing with users for the following interbank clearing and settlement systems was completed on 1 November 1998:

- Clearing House Automated Transfer System ("CHATS"), an interbank large value electronic payment system operated under a Real Time Gross Settlement mode, and the corresponding front-end terminal software;
- paper cheque system;
- electronic clearing system for low value bulk volume electronic payment items; and
- Central Moneymarkets Unit ("CMU") system, a central clearing and settlement system of public and private sector debt securities, and the corresponding front-end terminal software.

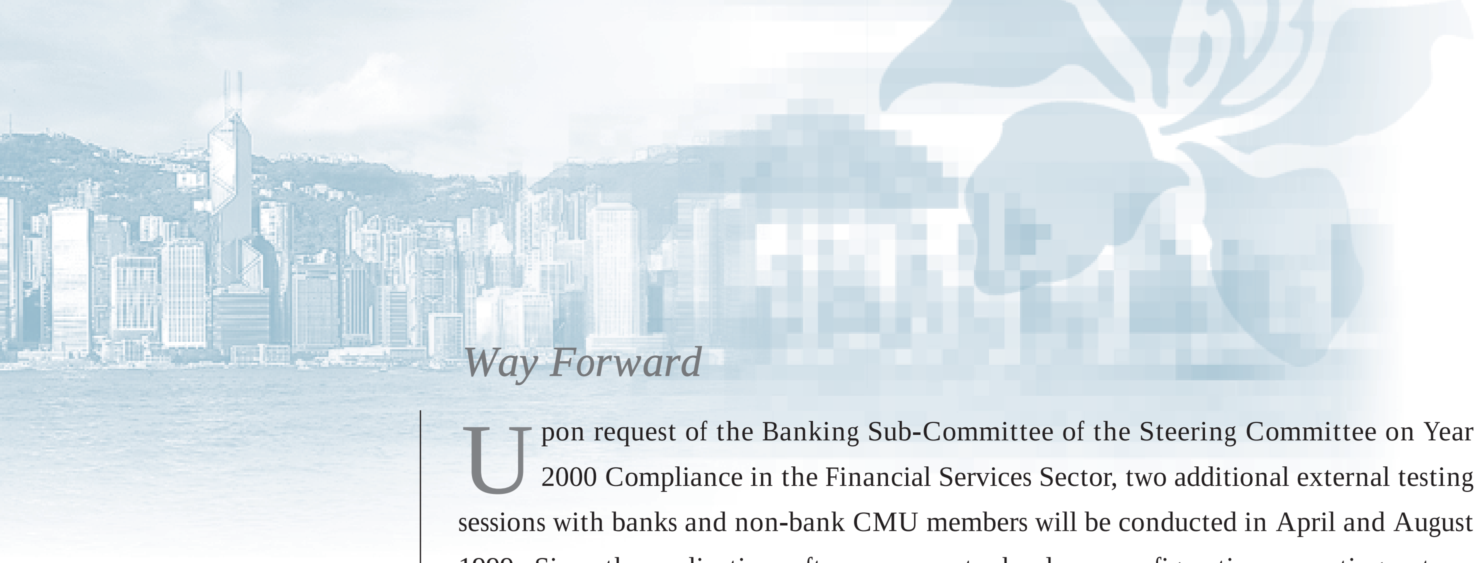
The external testing comprising 13 Year 2000 related dates was performed on most of the Sundays during 16 August 1998 to 1 November 1998. Banks with host application interface features and/or having electronic files exchanges with HKICL participated in all tests on a mandatory basis, whereas banks with no host application interface features and non-bank CMU users which are using homogenous hardware/software planforms participated in the tests on a rotational basis. All participants were requested to provide the test results to HKICL and confirmed that they had used their own Year 2000 compliant environment to execute the tests. Based on the test results received from the participants and HKICL's own record, no Year 2000 exceptions have been identified. Those users who for some reasons e.g. terminal system problem, telecommunication line failure, absence etc. could not successfully execute the test on certain test dates had requested re-tests, and four re-tests were arranged in November 1998. The positive re-test results confirmed by the requesting users had concluded the 13 test-dates external test.

HKICL has arranged with Hongkong Telecom to provide a Year 2000 compliant telecommunications test bed for the tests from 23 August 1998 to 1 November 1998. The dates of the test bed were adjusted in line with the Year 2000 test dates during the tests. Although the test bed was equipped with limited capacity, it satisfied the minimum requirement of different telecommunication line varieties. Both Hongkong Telecom and HKICL encountered no Year 2000 problems in the course of testing on the test bed.

Interface testing with the following business partners was completed with no Year 2000 exceptions reported:

- Hong Kong Securities Clearing Company for its Central Clearing and Settlement System ("CCASS") transactions including the real-time delivery vs. payments between CHATS and CCASS, CCASS participants' payments, and investor participants' payments;
- Electronic Payments Services Co. (HK) Limited ("EPSCO") for the clearing and settlement of Electronic Funds Transfer Point of Sales ("EFTPOS") transactions; and
- Joint Electronic Teller Services Limited ("JETCO") for the settlement of ATM transactions initiated from JETCO's ATM network.

HKICL will participate in the Global Financial Industry Year 2000 Test organised by the New York Clearing House in June 1999. A high level test plan is being prepared.



Way Forward

Upon request of the Banking Sub-Committee of the Steering Committee on Year 2000 Compliance in the Financial Services Sector, two additional external testing sessions with banks and non-bank CMU members will be conducted in April and August 1999. Since the application software, computer hardware configuration, operating systems software and telecommunication lines should have been verified and confirmed Year 2000 compliant, these additional tests are to be arranged mainly for HKICL and its users to ascertain that their systems including subsequent releases of enhancements are Year 2000 compliant. Participation will be voluntary.

These two tests will be conducted on a reduced scale and will only cover the turn of the century and the leap year of 2000. The test scope will include the majority of interbank clearing and settlement services i.e. CHATS, autopay, paper clearing, and CMU. However, interfaces with EPSCO, CCASS and JETCO clearing and settlements will be excluded, and no telecommunication test bed will be arranged.

The test schedule is shown below:

Year 2000 Test Dates	Dates of 1st Additional Testing (Sundays)	Dates of 2nd Additional Testing (Sundays)
31 December 1999	18 April 1999	8 August 1999
3 January 2000	25 April 1999	15 August 1999
4 January 2000	2 May 1999	22 August 1999
28 February 2000	9 May 1999	29 August 1999
29 February 2000	16 May 1999	5 September 1999
1 March 2000	23 May 1999	12 September 1999

HKICL has started the Year 2000 contingency planning and intends to complete the high level plan by end-December 1998, the detailed plan by end-March 1999 and the testing by end-September 1999.

Note by editor: updated monthly progress report of HKICL can be found at the web-site of the Year 2000 Steering Committee on Year 2000 Compliance in the Financial Services Sector at http://www.info.gov.hk/fsb/year2000/progress.doc.

Hope for the Best, Plan for the Worst - Year 2000 Contingency Planning

The Year 2000 problem is largely predictable in its timing, but highly unpredictable in its possible impact. Perhaps the greatest threat lies in this uncertainty. As a result, organisations are now realising that business contingency planning is a necessity, not a luxury. Tim Janes of PricewaterhouseCoopers discusses why Year 2000 business contingency planning requires a unique approach, and explains how organisations are focusing on Year 2000 business contingency as an essential component of the overall Year 2000 project.

However detailed and advanced an organisation's efforts to achieve Year 2000 compliance, it is likely that problems may arise due to circumstances that are completely beyond the control of the business and its management. In some cases it may be possible to rely on a manual fallback, as an alternative to disrupted IT-based procedures. In others, it may simply be the case of handling adverse media publicity. How can management who are responsible for the integrity of their companies' business operations ensure that appropriate measures are taken to address the threat, that despite all their best endeavours to "steer a safe course", the Year 2000 problem may still "collide" with the organisation?

Why Should The Year 2000 Be So Different?

It is understandable that companies in the financial services industry, which deal with all manner of risks on an everyday basis, might question the special attention that has been given to the Year 2000 problem. However, unlike many of the everyday risk factors, the Year 2000 bug is a pervasive and indiscriminate threat, which consequently generates a high degree of uncertainty about its impact. The Year 2000 bug may not manifest itself as an obvious or dramatic failure. A small date-based calculation error buried deep within a program could compound over time to create significantly greater problems. Systems may perform erratically or slowly, affecting processing times and productivity. Data corruption may undermine users' confidence in the quality of information available to them.

No matter how comprehensive your organisation's own Year 2000 plans may be, lack of preparation by a key supplier, customer or another third party could cause sudden and severe disruption to your business. A Gartner Group survey in 1998 revealed that 23% of the 15,000 firms surveyed had not yet started a Year 2000 project. Consequently, it is not inconceivable that there will be problems caused by inadequate preparations by a counterparty or supplier. In addition, there is the potential threat arising from systemic power and telecommunication network disruptions. If these partners provide indispensable input to your business, then you may inherit the consequences of their failure to prepare adequately for the Year 2000, threatening the stability and financial performance of your own organisation.

Even if your Year 2000 project is complete and successfully tested, will your customers share this confidence in your organisation's ability to sail through the Year 2000 storm? It will be important to maintain confidence in your organisation's products and services throughout the millennium transition period. A noticeable Year 2000 failure in a single financial institution could create negative perceptions about the integrity of the whole market. Even if nothing is wrong with your business, it may be necessary and prudent to communicate this fact to key customers and business partners. Silence may not be interpreted as a sign of self-confidence.

A common theme throughout all Year 2000 projects has been the need to deal with high levels of uncertainty. How big is the problem, how long will it take to fix and how much will it cost? The infallible answer has been, "you won't know until you start", closely followed by "and your initial estimates will probably be wrong". This degree of uncertainty will continue through and beyond the Year 2000 transition. Hence the need to develop effective and appropriate preparations to support business continuity in the event that the Year 2000 bug infects your business operations.

Don't Reinvent The Wheel

Before the Year 2000 problem was even a footnote in obscure IT magazines, many companies had already developed contingency arrangements to deal with the threat of IT or business disruption. Understandably, those companies are keen to maximise on their investment in time and resources by applying the established plans and preparations to the Year 2000 problem. Whilst this is a reasonable proposal, it needs to be approached with caution, and a clear understanding of the limitations of the existing plans.

In the past, a contingency plan was typically developed to respond to a diverse set of risks. The plan had to cope with a large number of possible hazards, such as loss of power, fire, or explosions, any of which could occur at an unpredictable time in the future. This fact necessarily imposed a broad-brush approach to the contingency preparations, so that they covered as many disaster permutations as possible.

By contrast, the Year 2000 problem allows an organisation to prepare for an event occurring at a known point (or points) in time, which will impact upon a definable set of resources and business processes. This provides the organisation with an opportunity to narrow down the range of threats that must be addressed, and develop contingency arrangements that are more focused. Key skills can be secured, and supporting resources acquired, for the risk periods.

Almost all existing contingency plans are built around the timely recovery of critical IT systems. A key strategic assumption is the ability of the recovery teams to conduct a prioritised restoration of critical IT systems at a designated recovery site within a defined time period.

Unfortunately, as unanticipated Year 2000 problems emerge, it may be the IT systems, software or hardware, that are the source of the disruption. Corrupted software will remain contaminated wherever it is installed, and the availability of a back-up server or "hot" recovery site is not much consolation.

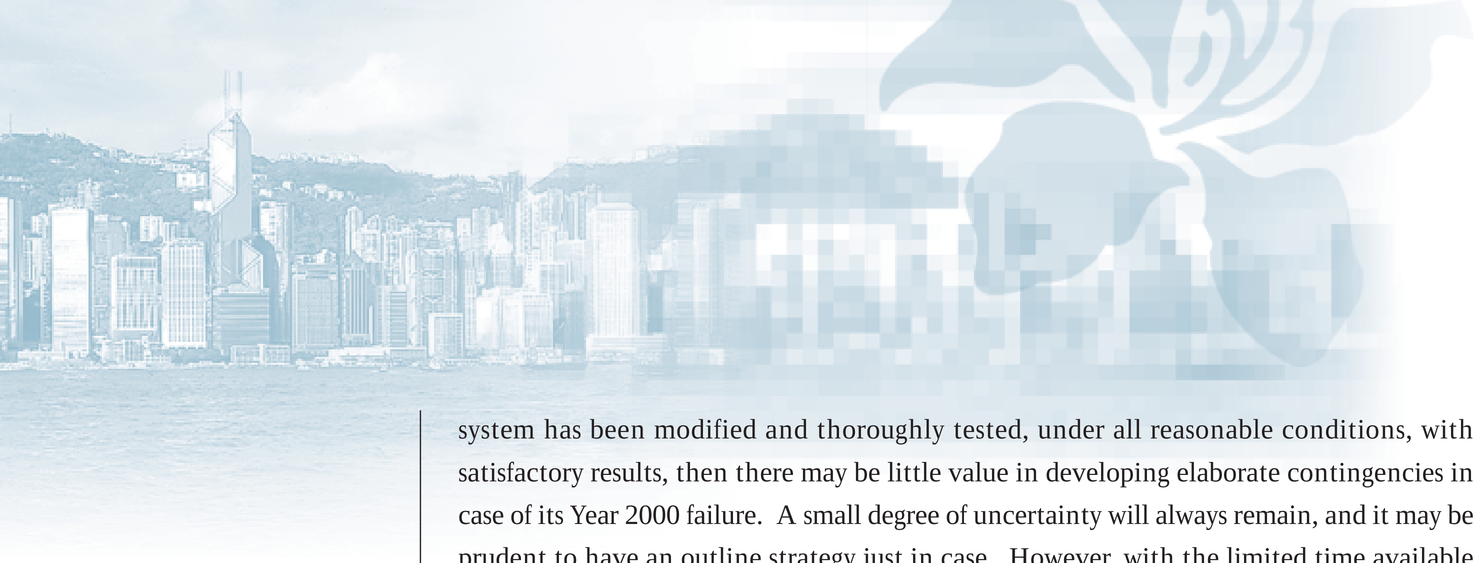
A further difference generated by the Year 2000 scenario arises from its uniform and indiscriminate nature. Traditional contingency plans assume that your organisation is the only party affected by the "disaster". With Year 2000, everybody will be threatened at the same time, including all the third parties your organisation trades with and depends upon. Aside from the organisation's own Year 2000 problems, external service providers, electronic data interfaces, suppliers, counterparties and key customers may represent the largest risk to business operations. Most conventional contingency plans do not generally consider non-functioning business partners.

Even if the Year 2000 limits the suitability of some established contingency arrangements, there are still many ways in which an existing contingency plan can be a valuable resource. The first and foremost is the acquired experience of the staff who developed and implemented the existing contingency plan. If they are not on the Year 2000 team, then they should be included as advisors for development of the plan. Proven emergency response and communication procedures can be reused, as can much of the reference information, such as staff and third party contact information. The basic format of the established contingency plan could become a template for the Year 2000 plan. In this way, companies may be able to re-colour the bulk of existing contingency plans with a Year 2000 shade. However, any recycling should be approached with caution; don't assume too much, or underestimate the specific risks created by the Year 2000 problem.

Reviewing The Risks

In the early stages of its Year 2000 project, an organisation should have conducted a risk assessment using its inventory of systems and equipment. From this assessment, modification and replacement strategies would have been determined, prioritised and implemented. As part of the contingency preparations this risk assessment should now be revisited. The basic questions remain, "how much will it hurt the business if it fails?", and "how certain am I that it will not fail?". Put another way, "what are the showstoppers and will they stop ?"

Fortunately, the risk assessment can now be conducted with the benefit of knowing what your Year 2000 programme has acceptably addressed, what remains to be fixed in the final months, and what resources will not be corrected in time. The results of the testing programmes should be factored into this risk assessment process. If a business critical IT



system has been modified and thoroughly tested, under all reasonable conditions, with satisfactory results, then there may be little value in developing elaborate contingencies in case of its Year 2000 failure. A small degree of uncertainty will always remain, and it may be prudent to have an outline strategy just in case. However, with the limited time available to develop contingency arrangements, it may be more effective to focus attention on systems and equipment which the Year 2000 team did not have time to fix, or where the confidence in the remedial efforts is less complete.

The same approach should be applied to business partners who have been questioned about their own Year 2000 remediation efforts. Your judgement of their ability to pass undisturbed through to the Year 2000 will be based on their ability and willingness to disclosure sufficient evidence of a sensible and realistic Year 2000 programme. If the evidence is not forthcoming; if there is a lack of transparency or co-operation; then the search for more “stable” trading partners, or alternative sources of supply should commence.

The risk assessment will not be a static process, unless you are fortunate to have completed each and every part of your Year 2000 project. As the project progresses, the Year 2000 compliance status of internal resources and external parties will change. As they do, the organisation’s Year 2000 risk exposure will evolve, and the contingency plans should adapt in response. There is an opportunity to concentrate contingency plans and preparations where they will have the most beneficial effect. Close monitoring of the progress of the Year 2000 programme, from the renovation of key systems to the compliance status of important business partners or vulnerable suppliers can help to ensure that contingency decisions are taken well in advance of a problem.

Strategies For Continuity

What are organisations actually proposing to do in the face of the Year 2000 threat? In a technology dependent industry, how far can financial services companies follow the low tech or no tech contingency route?

There is little evidence that the business world will come to a standstill at the dawn of the Year 2000, but there may be a deliberate slow down. Some companies will attempt to reduce the potential shock factor of the Year 2000 bug by reducing business volumes and minimising operating activity before and during the millennium transition period. They plan to do this by suspending non-essential business services, such as new account enquiries. Some business activities which would normally occur at month-end could be brought forward or deferred. For example, account statements that would normally be processed at the end of December 1999, or in early January 2000, could be issued in advance. However, it has to be recognised that this period is normally particularly busy for IT departments as the year end figures are processed. Careful planning and forethought will be required if traditional procedures are to be adapted to accommodate the Year 2000 threat.

Other protective strategies may also demand a change in work practices. Electronic data links between business partners may be temporarily disconnected, obliging staff to take on a great deal more manual data entry as a result. PC-based standalone applications may be brought in as a basic back-up to the usual network based systems. Some Financial Institutions have indicated that they will alter their trading strategies, to avoid settlement exposures during the Year 2000 transition period. Unfortunately, some firms may find themselves exposed to increased transaction volumes at exactly this time. Customers may demand to verify the status of their account balances as they empty accounts for emergency cash. As rumours multiply, investors may flock to move out of perceived high risk instruments, companies or countries for the security of lower risk investments, such as hard currencies or “quality” government bonds. Unanticipated market volatility may force Financial Institutions into reactive trading during this period.

In an effort to isolate Year 2000 problems from the mass of everyday IT failures, some organisations plan to impose a development freeze on all IT systems in the “danger zone” between September 1999 and 1st March 2000. This is planned to minimise the number of IT system errors, and allow those that do occur to be attributed to the Year 2000 problem and fixed quickly. In an effort to control the uncertain IT threat, other companies may implement a phased shut down of all IT systems prior to the event. Once the party is over, the IT systems will then be recovered in a controlled start up, managed by a specialised team, trained to run test programmes which will hunt for possible Year 2000 system problems. Of course, this strategy assumes that the organisation has IT systems that can be terminated without causing significant harm to ongoing business processes.

Such systematic analysis and early warning could be of great benefit for those organisations that operate on a global basis. Unfortunately, Hong Kong’s position in the global timezones means that it will be one of the first major financial centres to experience the Year 2000 effect. We may only receive a few hours advanced notice of problems from colleagues in Tokyo or Sydney. However, unselfish Year 2000 Teams in Hong Kong could give eight or thirteen hours early warning of impending Year 2000 problems to colleagues in London or New York.

The threat to commercial reputations may be the greatest concern for organisations that are confident of the success of their internal Year 2000 project. There is a real potential for rumour, confusion or mis-information to adversely affect market perceptions and undo all the good work of the last few years. Effective customer and media communications will be indispensable during the millennium transition. Public relations and customer call-centre staff will need to work closely with the Year 2000 team to maintain a current and accurate picture of the organisation’s Year 2000 status.

Plans and Preparations

Preparing the actual Year 2000 plan is the least difficult stage in the process, especially if the organisation has an existing contingency plan as a template. The detailed work begins once the high-level response strategies have been defined.

Detailed workaround procedures for essential, high-risk business processes should be created. The workaround procedures should assume that IT systems and data may not be available for prolonged periods. Key business partners and suppliers may also experience lengthy process interruptions. Viable and sustainable contingency solutions should be translated into detailed steps that will need to be followed in the event of Year 2000 failure. An example of a workaround procedure could involve the development of PC-based spreadsheets for manual capture of transaction information. Any manual procedures for critical business processes should be developed and tested by users to a stage where they are easy to interpret and ready to execute.

Some organisations propose to assemble Rapid Response Teams who will be available over the Year 2000 transition period. The team members, who have mostly been recruited from the Year 2000 project, must receive training and rehearsal time. Senior members of the team should be familiar with risk assessment and response strategies, so that the response to Year 2000 problems is considered and contingency plans are not invoked hastily.

Technical fix priorities should also be agreed in advance to avoid an ad-hoc approach to system fixes. They should define which systems have priority if several Year 2000 problems arise at once. Programmes and data should be prepared which will test the processing accuracy of “unaffected” systems and verify the quality of the output. Support staff may also need to be on hand to assist, possibly to enter data that usually arrived via external IT data interfaces, as some organisations may be unable, or unwilling, to exchange electronic transmissions. Other companies are establishing a Year 2000 command centre, populated with technical experts who will be employed to advise on fixing any systems that fail across a dispersed number of locations. Whichever approach is followed, to successfully assemble these teams and experts may require a combination of financial inducement and personal commitment. The members of the rapid response team are required to be on duty during the party of the century, and it will be of little use if half the team members are on the beach.

Finally, the procedures at the heart of the Year 2000 business contingency plan must be tested to confirm their feasibility and identify any teething problems. By participating in simulations of the workaround procedures, the process owners and users will gain comfort and confidence in the new work methods. A Business Contingency Plan is like a script for a play, if it hasn’t been rehearsed you don’t know if you have a triumph or a turkey.

One positive note amongst all the date-driven difficulties, is that the 31st December 1999 will fall on a Friday. The Year 2000 weekend will give Year 2000 Teams at least 48 hours to spot and rectify problems, or implement contingency arrangements, to support the start of business as usual on the first working day in January 2000.

Conclusion

The Year 2000 transition period will present a unique challenge for Financial Institutions. Certainly, Year 2000 failures pose a significant risk to business operations, but it is also a crisis situation that is predictable, allowing preparations to be made. The table below describes some of the key steps that should be considered in the development of a Year 2000 contingency plan.

The time available to fix all the Year 2000 problems is rapidly running out. Organisations should incorporate business contingency into their mainstream Year 2000 Programme. The reality is such that business contingency plans for the Year 2000 are not an option, they should be put in place now and tested - unless the procedures are rehearsed and people have practised them, the plans are not worth the paper they're printed on. A contingency plan is the last step in preparedness for the Year 2000 and provides final proof of due diligence in dealing with the potential risks. The truth is that no one can know exactly what problems will occur. Even the most optimistic commentators predict some degree of business disruption. Amidst the confusion, it makes sense to hope for the best but prepare for the worst.

Tim Janes is a Senior Manager in the Global Risk Management Solutions practice of PricewaterhouseCoopers in Hong Kong. He is responsible for Operational Risk Services, which include assisting clients to manage major technology threats such as the Year 2000 problem and business opportunities like the introduction of the Euro.

Note by editor: further references on Year 2000 contingency planning are available at the web-sites of US Federal Financial Institutions Examination Council at http://www.ffiec.gov/y2k/contplan.htm, US General Accounting Office at http://www.gao.gov/special.pubs/bcpguide.pdf, Bank of England at http://www.bankofengland.co.uk/y2t1098.htm, and Australian Bankers' Association at http://www.bankers.asn.au/.

Eight Steps Towards Developing a Year 2000 Contingency Plan

Contingency plans typically take the form of pre-planned alternative courses of action which are implemented when the main course of action begins to look unsuitable, to limit the potential damage. For example if an in-house Year 2000 system modification project begins to miss key milestones, you could install a standard off-the-shelf application as a replacement. More broadly, contingency plans may also include crisis response and operational recovery procedures to respond to uncertain or unknown events happening to an organisation. Here we outline the key steps that should be taken when developing your own Year 2000 Contingency Plan.

1. REVIEW THE YEAR 2000 PROJECT

Ensure the people responsible for the Year 2000 contingency plan are fully aware of the scope, current status and significant achievements of the Year 2000 project. Ideally, they should be part of the Year 2000 project team.

2. REVISIT RISK ASSESSMENTS

Review the original Year 2000 project risk assessment, bearing in mind that criticality ratings and contingency priorities for systems and resources may have changed, due to the achievements of the Year 2000 project.

3. DEVELOP YEAR 2000 STRATEGIES

Develop practical strategies for responding to anticipated Year 2000 problems. Capture opinions via workshops and interviews involving management and system users, and possibly key business partners and customers.

4. REVIEW EXISTING CONTINGENCY PLANS

Confirm existing contingency plans and recovery arrangements are applicable to the Year 2000 situation. Adapt and re-use the existing contingency plans where it is reasonable to do so, in order to save time and resources.

5. PREPARE THE PLANS AND SUPPORTING ARRANGEMENTS

Document action plans for responses to the specific Year 2000 problems defined previously, along with outline crisis management and communication procedures to deal with unanticipated situations that may arise.

6. ASSEMBLE THE PEOPLE

The Rapid Response Team should combine a mix of IT skills, business and Year 2000 experience. Team members must be willing and able to remain available over the Millennium Weekend.

7. TEST AND REHEARSE

Give the Year 2000 Team time to prepare and familiarise themselves with the documents and procedures that have been developed. Modify the plans based on lessons learnt during preparatory tests and simulations.

8. MONITOR AND MAINTAIN

The Contingency Plan can not be finished until the Year 2000 project is completed. Monitor the results of the Year 2000 project, and the compliance status of key business partners, and reflect major changes in the plan.