



Circulars

31 Jan 2002

Business Continuity Planning

Our Ref.: B1/15C

31 January 2002

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Business Continuity Planning

The HKMA has been reviewing the implications of the events of 11 September 2001 (9/11) for business continuity planning. Discussions on this issue have been held with banks, both individually and as a group, including those whose New York offices were directly affected by 9/11. In addition, the HKMA has conducted a self-assessment exercise involving 25 AIs in Hong Kong to gain an understanding of the effectiveness of their business continuity plans (BCPs).

This letter offers some preliminary conclusions on the lessons to be learned based on the work undertaken so far. The HKMA will however continue its research in this area, taking into account guidance being developed by the international regulatory community including the Financial Stability Forum. We will also step up our review of institutions' BCPs as part of our examinations of e-banking and information technology controls in 2002. It is also our intention to issue more detailed guidelines on business continuity planning later this year.

General lessons

There seems to be a general consensus that the main lessons to be drawn from 9/11 include the following:

- the increased level and intensity of the threats faced by banks and the need to cater for disasters that might involve complete destruction of key buildings and surrounding infrastructure, as well as loss of key staff;
- the risk of geographical concentration of key offices and back-up sites, complicated by the difficulty of getting physical access to back-up sites because of traffic disruption;
- the vulnerability of banks to breakdown of the telecommunications and power infrastructure;
- the need to deal with multiple events affecting service providers, counterparties and customers at the same time;

- the vulnerabilities of certain "choke points" of the financial system such as stock or futures exchanges, clearing firms and inter-dealer brokers, etc; and
- the need to be able to cope with prolonged disruptions and the importance of planning for business survival.

The state of readiness of BCPs in Hong Kong

This raises the issue of how well Als in Hong Kong could have coped with a disaster on the scale of 9/11. The self-assessment exercise referred to earlier suggests that there are a number of areas in which Als' BCPs could be improved. In particular, it appears that a number of Als may be relying on the efforts that they have previously put into their Y2K planning. However, too much reliance should not be placed on this. Y2K was a known event for which preparations could be made in advance (e.g. in terms of special back-up arrangements). It was also essentially a software problem and did not raise the issue of destruction of people and property.

Institutions should not therefore assume that their BCPs are adequate simply because plans were prepared for Y2K. Apart from anything else, it is necessary for such plans to be reviewed, updated and tested regularly. Als should therefore review their existing BCPs carefully in the light of a risk assessment of what they need to do to protect all the critical areas of their business under various scenarios. Given that BCPs involve a cost, this raises the question of what is the worst case scenario that Als should plan for. This is an extremely difficult question on which to advise and institutions will to some extent need to form their own judgement. However, it would seem sensible for Als to plan on the basis that they may have to cope with the complete destruction of buildings in which key offices or installations are located (rather than just denial of access for a period) and the loss of key personnel (including senior management)*. Als should also plan on the basis that the surrounding infrastructure (in particular power and telecommunications) may be affected and that back-up facilities might need to be used for an extended period of time.

In the light of this, Als may find it useful to consider two-tier plans: one to deal with short-term problems which would be fully developed with the physical capacity to put it into immediate effect and the other, which might be in paper form, to deal with a longer-term scenario (e.g. how to lease additional premises and how to accommodate processes that might not be critical immediately but would become so over time).

In developing, updating and testing BCPs it is important that the process should be endorsed and driven by top management. This is necessary to ensure that business continuity planning is taken seriously by all levels of staff and sufficient resources are devoted to putting the plan in place. Senior management should be aware of what they are personally required to do in the event of the BCP being invoked and should participate, where appropriate, in plan rehearsals which should be conducted, at a minimum, on an annual basis.

Specific lessons

Apart from the general lessons described above, there are a number of specific points of which Als should take note:

- Als should avoid placing excessive reliance on external vendors in providing BCP support, particularly where a number of institutions are using the services of the same vendor (e.g. to provide back-up facilities or additional hardware). Als should satisfy themselves that such vendors do actually have the capacity to provide the services when needed and the contractual responsibilities of the vendors should be clearly specified. The contractual terms should include the lead-time and capacity that vendors are committed to deliver in terms of back-up facilities, technical support or hardware. In some cases, a retainer agreement may be advisable to ensure priority service from the vendors in the face of competing demands from other affected users;
- Als should also check that important vendors themselves have effective BCPs;
- staff should be told clearly where they should go in an emergency, how do they get there and what do they do when they get there;
- this means that close attention needs to be given to the logistics of how to transport staff from the primary site to the back-up site, as well as from their homes in case the disaster strikes outside office hours. In addition, Als should ensure that alternate recovery personnel are identified for all critical processes. They should also participate in plan rehearsals to familiarise themselves with their recovery responsibilities;
- Als should establish a well-defined command centre structure and guidance should be given to staff as to how to communicate with the command centre in an emergency;
- contact numbers for key staff, counterparties, customers and service providers should be readily available to senior management and members of recovery teams (e.g. as wallet cards). Copies of the BCP document should be stored at locations separate from the primary sites. A summary of the key steps to take in an emergency should be made available to senior management and other key personnel and kept by them in multiple locations (e.g. office, home, briefcase, institution's website).
- Als should examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of back-up sites to primary sites. Key facilities should be sufficiently distanced to avoid being affected by the same disaster (e.g. they should be on separate telecommunication networks and power grids). The systems at back-up sites should be maintained and upgraded together with those in the primary sites. Recovery capacity may need to cater for processing volumes that exceed normal levels if, for example, more inquiries need to be handled;
- to cater for the fact that other parties may be affected by a disaster, Als should periodically test the ability of their back-up sites to communicate with the back-up sites of key counterparties, customers and service providers;
- there should be clear procedures in the BCP indicating how and in what priority vital records are to be retrieved or recreated in the event they are lost, damaged or destroyed;
- Als' BCPs should address the issue of how to handle media and PR issues to maintain public confidence in the event of disaster; and
- Als should incorporate the possible need to obtain additional liquidity into their BCPs.

The HKMA will be following up with individual Als on the steps they have taken to review and, where necessary, enhance their BCPs in the light of the events of 9/11. They are urged to treat this as a vital issue for business survival. The HKMA will also be liaising with the Financial Services Bureau and other regulators in Hong Kong on what further steps should

be taken to develop sector-wide contingency procedures and crisis management arrangements.

If you have any questions on the contents of this letter, please contact Shu-pui Li on 2878-1826 or Brian Lee on 2878-1651.

Yours faithfully

D T R Carse
Deputy Chief Executive

c.c Secretary for Financial Services
 The Chairman, The Securities and Futures Commission
 Commissioner of Insurance
 The Managing Director, The Mandatory Provident Fund Schemes Authority
 The General Manager, The Hong Kong Interbank Clearing Limited

*This need not be caused by a terrorist attack. It could be the result of, e.g. a serious fire.

Last revision date : 01 August 2011