HONG KONG MONETARY AUTHORITY 香港金融管理局		
Supervisory Policy Manual		
TM-G-2	**Business Continuity Planning**	V.2 – Consultation ~~V.1 – 02.12.02~~

This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To set out the HKMA's supervisory approach to business continuity planning and the sound practices which the HKMA expects AIs to take into consideration in this regard

Classification

A non-statutory guideline issued by the MA as a guidance note

Previous guidelines superseded

TM-G-2 "Business Continuity Planning" (V.1) dated 02.12.02

~~This is a new guideline.~~

Application

To all AIs

Structure

1. Introduction
   - 1.1 Terminology
   - 1.2 Scope of business continuity planning
   - 1.3 Supervisory approach
2. Board and senior management oversight
   - 2.1 Establishment of policy, process and responsibility
   - 2.2 Monitoring and reporting
3. Business impact analysis and recovery strategy
   - 3.1 Business impact analysis
   - 3.2 Recovery strategy formulation

4. Development of Business Continuity Plan
- 4.1 Overview
- 4.2 Crisis management process
- 4.3 Business resumption
- 4.4 Technology recovery
- 4.5 Business continuity models
- 4.6 Vital record management
- 4.7 Public relations and communication strategy
- 4.8 Other risk mitigating measures

5. Alternate sites for business and technology recovery
- 5.1 Selection criteria for alternate sites
- 5.2 Alternate sites for technology recovery
- 5.3 Alternate sites provided by vendors or other institutions

6. Implementation of Business Continuity Plan
- 6.1 Testing and rehearsal
- 6.2 Periodic maintenance

---

1. Introduction

1.1 Terminology

1.1.1 In this module:

- "business continuity planning" refers to the advance planning and preparations which are necessary to identify the impact of potential losses arising from an emergency or a disaster; to formulate and implement viable recovery strategies; to develop recovery plans which ensure continuity of an AI's operations~~services~~ in that relation; and to administer a comprehensive testing and maintenance programme;
- "Business Continuity Plan ("BCP")" refers to a collection of procedures and information which is

developed, compiled and maintained in readiness for use in the event of an emergency or disaster;

- "business impact analysis" refers to a management level analysis which identifies and assesses the impact of losing the various functions and services within an AI. The impact analysis tries to measure the potential loss and escalating losses over time in order to provide senior management with reliable data for the identification of critical operations~~services~~. Based on the results of the analysis, the AI should be able to identify the scope of the critical operations~~services~~ to be provided and the time-frame in which the operations~~services~~ should be resumed;
- "call-out tree" refers to a pre-defined sequence of points of contact of staff for dissemination of information;
- "crisis management team ("CMT")" refers to a group of executives who would direct the recovery operations while taking responsibility for the survival and the reputation of the AI;
- "Critical operations" refers to: (i) activities, processes, and services performed by an AI, as well as (ii) the supporting assets (including people, technology, information and facilities) necessary for the delivery of such activities and services, which if disrupted, could pose material risks to the viability of the AI itself or impact the AI's role within the Hong Kong financial system[1]. AIs should refer to "OR-2 Operational Resilience" for more details about this term.
- "crisis management" refers to the overall process designed to support the CMT when dealing with a specific emergency situation which might threaten the operations, staff, customers or reputation of an AI; and

[1] These should include any "critical financial functions", as defined in the Code of Practice "CI-1 Resolution Planning – Core Information Requirements", that may be performed by the AI.

- "recovery strategy" refers to a strategy to resume the minimum set of critical operations~~services~~ identified in the business impact analysis (e.g. use of another delivery channel to provide the same operation~~service~~).
- "Severe but plausible scenarios" refers to situations that would result in significant disruptions, and while unlikely to occur, remain probable. AIs should refer to "OR-2 Operational Resilience" for more details about this term.
- "Tolerance for disruption" refers to the maximum level of disruption to a critical operation that an AI can accept. AIs should refer to "OR-2 Operational Resilience" for more details about this term.

1.2 Scope of business continuity planning

1.2.1 This module should be read in conjunction with "OR-2 Operational Resilience" with respect to the purposes of ensuring critical operations delivery and AIs should ensure that they are compliant with the relevant requirements specified therein.

~~1.2.1~~1.2.2 The destruction of buildings, loss of life, and the widespread dislocations to financial institutions' operations resulting from the incident of 11 September, 2001 ("9/11") have prompted many institutions to review their scope of business continuity planning. It is clear that the traditional scope of business continuity planning for inaccessibility of a single building for a short period is not adequate.

~~1.2.2 Efforts put into, and experiences gained from the preparation of, the Y2K contingency plan were obviously not sufficient to cope with 9/11. Y2K was a known event and was essentially a software problem. Also, it did not raise the issue of destruction of people and property.~~

1.2.3 The HKMA recognises that BCPs involve a cost, and that it may not be cost effective to have a fully developed and implemented plan for all the worst case scenarios. However, having regard to past events, it would seem sensible for AIs to plan on the basis that they may have to cope with the complete destruction of buildings and surrounding infrastructure in which their key offices,

installations, counterparties or service providers are located, the loss of key personnel, and the situation that back-up facilities might need to be used for an extended period of time.

1.2.4 AIs may find it useful to consider two-tier plans: one to deal with near-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).

1.2.5 Depending on the individual circumstances of AIs, the longer-term plan may include plans on how to reconstruct the primary sites or to move to a new permanent work location. For example, this may require that duplicates of design documents, floor plans and cabling diagrams should be kept off-site.

1.3 Supervisory approach

1.3.1 The HKMA's supervisory objective is to help ensure that AIs have workable and well thought through BCPs to protect all the critical areas of their business and to cope with prolonged disruptions.

1.3.2 The HKMA will, in the course of its on-site examinations, off-site reviews and prudential meetings with AIs, determine as appropriate the adequacy of their efforts being put into business continuity planning. In assessing the adequacy of AIs' BCP, the HKMA will have regard to the practices set out in this module.

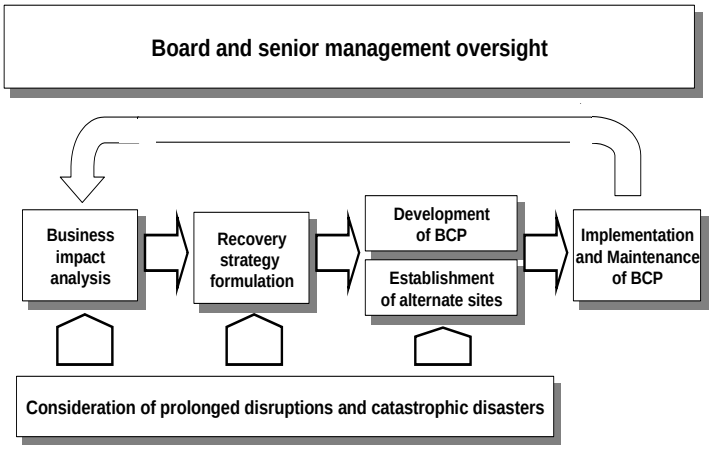
1.3.3 AIs should inform the HKMA promptly if their BCP is activated. The HKMA should also receive periodic progress reports upon being notified until the final resolution of the crisis.

2. Board and senior management oversight

2.1 Establishment of policy, process and responsibility

2.1.1 The Board of Directors[2] and senior management of AIs have the ultimate responsibility for business continuity planning and the effectiveness of their BCP. The senior management should establish policies, standards and processes for business continuity planning[3], which should be endorsed by the Board. The senior management should ensure that business continuity planning is taken seriously by all levels of staff and that sufficient resources are devoted to implementing the plan.

2.1.2 In this module, the suggested process for business continuity planning consists of several key components as shown in the following diagram:



The senior management should establish clearly which function in the institution has the responsibility for managing the entire process of business continuity planning -(the BCP function).

2.2 Monitoring and reporting

[2] For the purpose of this module, the responsibility of Board oversight of business continuity planning for overseas incorporated AIs in respect of Hong Kong operation should rest with the local senior management.

[3] In developing the policies, standards and processes for business continuity planning, AIs may find it useful to draw additional reference from some of the BCP resources, e.g. the Business Continuity Institute: "www.thebci.org" and the Disaster Recovery Institute: "www.drii.org".

2.2.1 The BCP function should submit regular reports to the Board and senior management on the testing of its BCP. Any major changes to the BCP should also be reported to the senior management.

2.2.2 The internal audit function of an AI should conduct periodic review of its BCP to determine whether the plan is realistic and remain relevant, and whether it adheres to the policies and standards established by the AI.

2.2.3 Given the importance of business continuity planning, the Chief Executive of AIs should prepare and sign-off a formal annual statement submitted to the Board on whether the recovery strategies adopted are still valid and whether the documented BCPs are properly tested and maintained. The annual statement should be incorporated into the BCP and will be reviewed as part of the HKMA's on-site examinations.

3. Business impact analysis and recovery strategy

3.1 Business impact analysis

3.1.1 The objective of the business impact analysis is to identify different kinds of risks to business continuity and to quantify the impact of disruptions. The business impact analysis helps to identify those critical business activities, banking services and internal support functions which, in the event of a disaster, must be consistently and effectively delivered by an AI.

3.1.2 The business impact analysis normally comprises two stages. The first stage is to identify critical operations~~services~~ that must be maintained and continued in the event of a disaster. This usually entails an assessment of the overall exposure to the AI if the normal functions or services cannot be performed. The criteria for the assessment include the impact on customers, personnel, reputation and internal services as well as the financial and legal implications. The second stage is a time-frame assessment. It aims to determine how quickly the AI needs to resume the critical ~~functions or services~~operations identified, taking into account the tolerance for disruption set by the AI.

3.1.3 Based on the business impact analysis, the business and support functions should be able to define the minimum level of critical operations~~services~~ to be delivered in the event of a disaster.

3.2 Recovery strategy formulation

3.2.1 Individual critical business and support functions should formulate their own recovery strategies on how to achieve the recovery time-frame and to deliver the minimum level of critical operations~~services~~ derived from the business impact analysis. This involves determination of an alternate site, total number of recovery personnel and the related workspace, applications and technology requirements, office facilities and vital records required for the provision of such levels of operations~~services~~. AIs should take note that they might need to cater for processing volumes that exceed those under normal circumstances.

3.2.2 The result of the time-frame assessment in the business impact analysis is the key determination factor for the recovery priority of individual services. The inter-dependency among critical operations~~services~~ is another major consideration in determining the recovery strategies and priority. For example, the recovery of the front office operations is highly dependent on the recovery of the middle office and back office support functions.

3.2.3 Having performed the business impact analysis and formulated the recovery strategies, individual critical business and support functions should have established the minimum BCP requirements for the provision of essential business and technology services levels. To avoid any unnecessary arguments and inappropriate BCP investment at a later stage, these BCP requirements should be approved by the senior management prior to proceeding to the development of the BCP. In addition, senior management should also ensure that the business continuity requirements should be considered at the planning and development stages of new business products and services.

4. Development of Business Continuity Plan

4.1 Overview

4.1.1 Once the recovery strategies for individual business and support functions are determined and the BCP requirements are finalised, the development of the BCP should commence. The objective of the BCP is to provide detailed guidance and procedures to respond to and manage a crisis, to resume and continue critical operations~~business services and functions~~ identified in business impact analysis, and to ultimately return to business as usual.

4.1.2 An effective BCP is forward-looking, and should be validated for a range of severe but plausible scenarios which contain disruptive events and incidents. The BCP should identify critical operations as well as the key internal and external dependencies supporting these critical operations. It should incorporate business impact analysis, recovery strategies, testing programmes, training and awareness programmes, communication strategies and crisis management processes. An AI's BCP for the delivery of critical operations, including those reliant on critical third-party services, should be consistent with its operational resilience framework. The same consistency requirement also applies to BCPs which may be contained within an AI's recovery and resolution plans.

~~4.1.1~~4.1.3 AIs should perform documentation of their BCP along with the development of the recovery organisation, procedures and arrangements. The BCP documentation and development should not be treated as two unrelated and independent projects. Otherwise, it may be difficult to ensure that the content of the BCP is consistent with the actual recovery processes and arrangements. The BCP development process is summarised below.

4.2 Crisis management process

4.2.1 It is important to note that a disaster will evolve after occurrence. AIs should establish a CMT to respond to and manage the various stages of a crisis. The CMT should comprise members of the senior management and heads of major support functions (e.g. building facilities, IT, corporate communications and human resources).

4.2.2 BCPs should set out a crisis management process that serves as documented guidance to assist senior management in dealing with and containing an emergency to avoid spillover effects to the business as a whole. Senior management should identify potential crisis scenarios and where applicable develop specific crisis management procedures for managing these scenarios (i.e. a procedure to handle a bomb threat is different from that to handle a major power failure). The overall crisis management process, at a minimum, should contain the following:

- the process for ensuring early detection of an emergency or a disaster and prompt notification to the CMT about the incident;
- the process for establishing the roles and responsibilities for managing operational disruptions and clear guidance regarding the succession of authority in the event of a disruption that impacts key personnel;
- the process for the CMT to assess the overall impact on the AI and to make quick decisions on the appropriate responses for action (i.e. staff safety, incident containment and specific crisis management procedures);
- the arrangements for safe evacuation from business locations (e.g. directing staff to pre-arranged emergency assembly area, taking attendance of all employees and visitors and tracking missing people through different means immediately after the disaster);
- clear internal decision-making process and ~~clear~~ criteria for activation of the BCP and/or alternate sites;
- the process for gathering updated status information for the CMT (e.g. ensuring that regular conference calls are held among key staff from relevant business and support functions to report on the status of the recovery process);
- the process for timely internal and external communications (see subsection 4.7 below); and

- the process for overseeing the recovery and restoration efforts of the affected facilities and the business services.

4.2.3 If CMT members need to be evacuated from their primary business locations, AIs should set up command centres to provide the necessary workspace and facilities for the CMT. Command centres should be sufficiently distanced from AIs' primary business locations to avoid being affected by the same disaster.

4.3 Business resumption

4.3.1 Each relevant business and support function should establish a business recovery team which may have sub-teams to carry out the business resumption process. Appropriate recovery personnel with the required knowledge and skills should be assigned to the teams. AIs should ensure that alternate recovery personnel are identified for all critical processes. Contact numbers for recovery and alternate personnel, including contact information after office hours, should be available for an emergency (e.g. as wallet cards). AIs should also consider a staff rotation plan in order to cover extended working hours for business recovery.

4.3.2 Generally, the business resumption process consists of three major phases:

- The mobilisation phase – This phase aims to notify the recovery teams (e.g. via a call-out tree) and to secure the resources (e.g. recovery services provided by vendors) required to resume business services. This phase might involve determination of the sequence for restoring business services if it needs to be different from the pre-determined sequence in the BCP;
- The alternate processing phase – This phase emphasises the resumption of the business and service delivery at the alternate site and/or in a different way than the normal process. This may entail record reconstruction and verification, establishment of new controls, alternate manual processes, and different ways of dealing with customers and counterparties; and

- The full recovery phase – This phase refers to the process for moving back to a permanent site after a disaster. It is as difficult and critical to the business as the process to activate the BCP.

4.3.3 For the first two phases, clear responsibilities should be established and activities prioritised. A recovery tasks checklist should be developed and included in the BCP. It is recognised that certain tasks involved in the full recovery phase may depend on the nature of the disaster concerned and that it may be difficult to formulate detailed plans in advance. However, the BCP should at least identify and plan for activities which would be required in any events, for example, the verification of the safety and readiness of the permanent site.

4.4 Technology recovery

4.4.1 Business resumption very often relies on the recovery of technology resources that include applications, hardware equipment and network infrastructure as well as electronic records. The technology requirements that are needed during recovery for individual business and support functions should be specified when the recovery strategies for the functions are determined.

4.4.2 AIs should pay attention to the resilience of critical technology equipment and facilities such as the Uninterruptible Power Supply ("UPS") and the cooling systems. Such equipment and facilities should be subject to continuous monitoring and periodic maintenance and testing. This would reduce the probability of having to activate the BCP and the inevitable disruptions to normal business.

4.4.3 Appropriate personnel should be assigned with the responsibility for technology recovery. Alternate personnel needs to be identified for key technology recovery personnel in case of their unavailability to perform the recovery process.

4.5 Business continuity models

4.5.1 There are various business continuity models that could be adopted by AIs to handle prolonged disruptions. The traditional model is an "active/back-up" model, which is widely used by many organisations. This traditional

model is based on an "active" operating site with a corresponding alternate site (back-up site), both for data processing and for business operations. This model may require significant investment if the "back-up site" needs to be equipped to support for prolonged disruptions of the "active site".

4.5.2 An emerging split operations model, which has already been used by some institutions, is a different business continuity model. This model is to operate with two or more widely separated active sites for the same critical operations, providing inherent back-up for each other (e.g. call centres for customer services). Each site has the capacity to take up some or all of the work of another site for an extended period of time. This strategy can provide nearly immediate resumption capacity and is normally able to handle the issue of prolonged disruptions.

4.5.3 The split operations model may incur higher operating costs, in terms of maintaining excess capacity at each site and added operating complexity. It may be difficult to maintain appropriately trained staff and pose technological issues at multiple sites.

4.5.4 The question of what business continuity model to adopt is for individual institutions' judgement based on the risk assessment of their business environment and the characteristics of their own operations.

4.6 Vital record management

4.6.1 Each BCP should clearly identify information deemed vital for recovery of critical business and support functions in the event of a disaster and the relevant protection measures. Vital information includes that stored on both electronic or non-electronic media (e.g. paper records).

4.6.2 Copies of vital records should be stored off-site as soon as possible after creation. Back-up vital records must be readily accessible for emergency retrieval. Access to back-up vital records should be adequately controlled to ensure that they are reliable for business resumption purposes. For certain critical operations~~services~~, AIs should consider the need for instantaneous data back-up (e.g. adopting real-time data mirroring technology) to

ensure prompt system and data recovery. There should be clear procedures indicating how and in what priority vital records are to be retrieved or recreated in the event that they are lost, damaged or destroyed.

4.7 Public relations and communication strategy

4.7.1 AIs should formulate a formal strategy for communication with key external parties (e.g. regulators, investors, customers, counterparties, business partners, service providers, the media and other stakeholders). The strategy needs to set out to which parties AIs should communicate in the event of a disaster. This will ensure that consistent and up-to-date messages are conveyed to the relevant parties. During a disaster, ongoing and clear communication is likely to assist in maintaining the confidence of customers and counterparties as well as the public in general.

4.7.2 The BCP should clearly indicate who can speak to the media, and have pre-arrangements for redirecting external communications to designated staff during a disaster. AIs may find it helpful to prepare draft press releases as part of their BCP. This will save the CMTs' time in determining the main messages to convey in a chaotic situation. Important conversations with external parties should be properly logged for future reference. Important contact numbers and e-mail addresses of key external parties should be kept in a readily accessible manner (e.g. in wallet cards or AIs' intranet).

4.7.3 As regards internal communication, the BCP should set out how the status of recovery can be promptly and consistently communicated to all staff, parent bank, head office, branches and subsidiaries, where appropriate. This may entail the use of various communication channels (e.g. broadcasting of messages to mobile phones of staff, AIs' websites, e-mails, intranet and instant messaging).

4.8 Other risk mitigating measures

4.8.1 AIs should have proper insurance coverage to reduce the financial exposure that they may face during a disaster. AIs should regularly review the adequacy and coverage of their insurance policies in reducing any

foreseeable risks caused by disasters, such as loss of offices, critical IT facilities and equipment, and casualty. Insurance policies may also need to address AIs' legal responsibilities for failing to deliver services to their customers and counterparties.

4.8.2 AIs should also incorporate the possible need to obtain additional liquidity into their BCPs.

5. Alternate sites for business and technology recovery

5.1 Selection criteria for alternate sites

5.1.1 Most business continuity efforts are dependent on the availability of an alternate site (i.e. recovery site) for successful execution. The alternate site may be either an external site available through an agreement with a commercial vendor or a site within the AI's real estate portfolio. A useable, functional alternate site is an integral component of all BCPs.

5.1.2 AIs should examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of the alternate sites to primary sites. Alternate sites should be sufficiently distanced to avoid being affected by the same disaster (e.g. they should be on separate or alternative telecommunication networks and power grids).

5.1.3 AIs' alternate sites should be readily accessible and available for occupancy (i.e. 24 hours a day, 7 days a week) within the time requirement specified in their BCPs. Should the BCPs so require, the alternate sites should have pre-installed workstations, power, telephones and ventilation, and sufficient space. Appropriate physical access controls such as access control systems and security guards should be implemented in accordance with AIs' security policy.

5.1.4 Other than the establishment of alternate sites, AIs should also pay particular attention to the transportation logistics for relocation of operations to alternate sites. Consideration should be given to the impact a disaster may have on the transportation system (e.g. closures of roads or tunnels). Some staff may have difficulty in commuting from their homes to the alternate sites. Other

logistics, such as how to re-route internal and external mail to alternate sites should also be considered. Moreover, pre-arrangement with telecommunication companies for automated telephone call diversion from the primary work locations to the alternate sites should be considered.

5.2 Alternate sites for technology recovery

5.2.1 Alternate sites for technology recovery (i.e. back-up data centres), which may be separate from the alternate business site, should have sufficient technical equipment (e.g. workstations, servers, printers, etc.) of appropriate model, size and capacity to meet recovery requirements as specified by AIs' BCPs. The sites should also have adequate telecommunication (including bandwidth) facilities and pre-installed network connections as specified by their BCPs to handle the expected voice and data traffic volume.

5.2.2 AIs should consider arranging telecommunication links from their alternate sites to the alternate sites of major customers, counterparties and service providers whose primary sites are close to AIs' primary business locations and who may therefore be affected by the same disaster being catered for. Priority should be given to establishing telecommunication links to those parties upon which AIs' critical operations~~services~~ have a high dependency.

5.3 Alternate sites provided by vendors or other institutions

5.3.1 AIs 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). AIs 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.

5.3.2 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. The vendor should be able to demonstrate its own recoverability including the specification of another recovery site in the event that the contracted site becomes unavailable.

5.3.3 Certain AIs may rely on a reciprocal recovery arrangement with another institution to provide recovery capability. AIs should, however, note that such arrangement is often not appropriate for prolonged disruptions and an extended period of time. This arrangement could also make it difficult for AIs to adequately test their BCP. Any reciprocal recovery agreement should therefore be subject to proper risk assessment and documentation by AIs, and formal approval by the Board.

6. Implementation of Business Continuity Plan

6.1 Testing and rehearsal

6.1.1 AIs should not consider their BCP as complete if the plans have not been subject to proper periodic testing. Testing is needed to ensure that the BCP is operable. Testing of BCP should be conducted and validated for a range of severe but plausible scenarios that incorporate disruptive events and incidents. Testing entails verifying the awareness and preparedness of AIs' personnel as well as determining how well the BCP really works.

6.1.2 AIs are expected to conduct testing of their BCP at least annually. Senior management should participate in the annual testing and be aware of what they are personally required to do in the event of their BCP being invoked. In addition, both recovery and alternate personnel should participate in plan rehearsals to familiarise themselves with their recovery responsibilities.

6.1.3 All BCP related risks and assumptions must be reviewed for relevancy and appropriateness as part of the annual planning of testing. The scope of testing should be comprehensive to cover the major components of the BCP as well as coordination ~~and interfaces~~ among important parties, and interdependencies with third

parties and intragroup entities. Depending on the testing objectives and parties involved, the types of BCP testing may include a desk-top structured walkthrough, a testing of particular components of the BCP or a fully integrated testing[4]. In particular:

- staff evacuation and communication arrangements (e.g. call-out trees) should be validated;
- the alternate sites for business and technology recovery should be activated;
- important recovery services provided by vendors or counterparties should form part of the testing scope;
- AIs should consider testing the linkage of their back-up IT systems with the primary and back-up systems of key customers, counterparties and service providers;
- if back-up facilities are shared by other parties (e.g. subsidiaries of the institution), the AI needs to verify whether all parties can be accommodated concurrently; and
- recovery of vital records should be certified as part of the testing.

6.1.4 Formal testing documentation (including testing plan, testing scenarios, testing procedures and testing results) should be produced to ensure thoroughness and effectiveness of testing. Specifically, a post mortem review report should be prepared at the completion of the testing for formal sign-off by AIs' senior management. If the testing results indicate a weakness or gap in the BCP, the plans and recovery strategies should be updated to remedy the situation.

6.2 Periodic maintenance

6.2.1 AIs should have formal change management procedures to keep their BCPs updated in respect of any relevant

[4] In a fully integrated testing, every facet of the BCP is tested together. This test is usually performed during non-business hours to avoid disrupting normal operations and customers.

changes with proper approval and documentation. In the event that a plan has been activated, a review should be carried out once normal operations are restored to identify areas for improvement. If vendors are needed to provide vital recovery services, there should be formal processes for regular (say, annual) reviews of the appropriateness of the relevant service level agreements.

6.2.2 Individual business and support functions, with the assistance of the BCP function, should review their business impact analysis and recovery strategy, say on an annual basis. This aims to confirm the validity of, or whether updates are needed to, the BCP requirements (including the technical specifications of equipment of the alternate sites) for the changing business and operating environment.

6.2.3 The contact information for key staff, counterparties, customers and service providers should be updated as soon as possible when notification of changes is received.

6.2.4 Significant internal changes (e.g. merger or acquisitions, business re-organisation or departure of key personnel) should be reflected in the plan immediately and reported to senior management.

6.2.5 Copies of the BCP document should be stored at locations separate from the primary sites. A summary of 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 or AI's website).