澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

Circular No. 033/B/2009-DSB/AMCM
(Date: 14/8/2009)

Guideline on Business Continuity Management

The Monetary Authority of Macao (AMCM), under the powers conferred by Article 9 of the Charter approved by Decree-Law No.14/96/M of 11th March and by Article 6 of the Financial System Act of Macao approved by Decree-Law No. 32/93/M of 5th July, establishes the following:

Introduction

1. Past events in other parts of the world showed that system failures, computer malfunction, natural disasters, outbreak of infectious diseases, acts of terrorism and many other incidents could lead to major operational disruption in the financial industry. These heighten business continuity (i.e. a state of continued, uninterrupted operation of a business) as an ongoing priority for credit institutions and demonstrate the need for credit institutions to have robust business continuity arrangements.

2. In order to minimise the financial, legal, reputational and other material consequences arising from disruptions, credit institutions are expected to have effective business continuity management (BCM), which is defined as a comprehensive approach that includes policies, standards and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Such approach should address both the technical considerations and human dimension and, the personal safety of staff should be the paramount consideration. Credit institutions are also expected to incorporate BCM as an ongoing process and as part of the planning phase for new business, material outsourcing arrangements and major projects involving the introduction of new business processes and systems.

3. To ensure that effective BCM is implemented by credit institutions[1], this Guideline sets forth the essential principles and key processes of BCM and the supervisory approach that the AMCM will take in assessing the adequacy of credit institutions' BCM. In particular, the AMCM expects all credit institutions to develop and implement workable and effective business continuity plans (BCPs) that are consistent with the nature and scale of their

[1] These include overseas branches of credit institutions incorporated in Macao and Macao branches of credit institutions incorporated overseas.

operations. Where applicable, this Guideline also applies to other financial institutions (excluding institutions that transact insurance activities and/or manage private pension funds) that are under the supervision of the AMCM. However, those financial institutions whose transactions with customers can be completed on-the-spot are less likely to be called upon to comply with this Guideline.

BCM Principles and Processes

4. On the basis of the principles recommended by the Joint Forum[2] in its paper of August 2006 "High level principles for business continuity" (http://www.bis.org/publ/joint17.pdf), the AMCM sets forth the following BCM principles for adoption by credit institutions:

   Principle 1: Board and senior management responsibility:

   Credit institutions should have effective and comprehensive approaches to BCM. A credit institution's board of directors[3] (the board) and senior management are collectively responsible for the institution's business continuity.

   Principle 2: Major operational disruptions:

   Credit institutions should explicitly consider and plan for major operational disruptions and incorporate the risk of such disruptions into their approaches to BCM.

   Principle 3: Recovery objectives:

   Credit institutions should develop recovery objectives that reflect the risk they represent to the operation of the financial system.

   Principle 4: Communications:

   Credit institutions should include in their BCPs procedures for internal communications and for communicating with relevant external parties, including external parties in other jurisdictions, in the event of a major operational disruption.

---

[2] The Joint Forum comprises the following standard setting bodies: the Basel Committee on Banking Supervision, the International Organisation of Securities Commissions and the International Association of Insurance Supervisors.

[3] In the case of branches of overseas incorporated credit institutions, the reference to "the board of directors / the board" in this Guideline refers to, depending on the circumstances, either the branches' local management or, the management at the head offices responsible for the operations of the branches.

Principle 5: Testing:

Credit institutions should test their BCPs, evaluate their effectiveness, and update their BCM, as appropriate.

5. The above principles are set forth by the AMCM on the understanding that an effective BCM framework will involve an integration of a number of processes. Typically, these processes include:

(a) risk identification and assessment;

(b) business impact analysis;

(c) recovery strategies;

(d) business continuity planning;

(e) communications;

(f) testing;

(g) training and awareness;

(h) crises management;

(i) updating BCPs;

(j) audit and independent reviews; and

(k) insurance consideration.

6. The general requirements and recommended practices of the above BCM processes and the responsibility of a credit institution's board and senior management in steering the integration of these processes are given in more details under paragraphs 7 to 38 of this Guideline. In addition to the guidance given in this Guideline, credit institutions in developing their BCM framework may also wish to draw reference from the Joint Forum's paper as well as from other BCM organisations or private sector groups[4]. For example, they could find from Annexes I to V of the Joint Forum's paper some relevant case studies[5] on recent instances of major operational disruptions.

---

4 Examples of BCM organizations and private sector groups include The Disaster Recovery Institute International (www.drii.org), The Business Continuity Institute (www.thebci.org), The Security Industry Business Continuity Management Group (www.sia.com) and ChicagoFIRST (www.chicagofirst.org) etc.

5 The case studies include: (i) US-Canadian electrical power grid outages in August 2003; (ii) The impact of the 2003 SARS outbreak on Hong Kong SAR's securities markets; (iii) The impact of the 2003 SARS outbreak on the Canadian securities industry; (iv) Niigata Chuetsu earthquake; and (v) The London terrorist attacks on 7 July 2005.

General Requirements and Recommended Practices on BCM Processes

Board and Senior Management Responsibility:

7. A credit institution's board and senior management are responsible for managing the institution's business continuity effectively.

8. The board and senior management are expected to fulfil their business continuity responsibilities by setting policies, prioritizing critical business functions, allocating sufficient resources and personnel, providing oversight, approving BCP / BCPs, reviewing test results and ensuing maintenance of a current BCP. Such responsibility on BCM also covers business operations that have been outsourced to other service providers. The board and senior management should also create and promote an institutional culture that places a high priority on business continuity. The provision of sufficient financial and human resources should help with this objective.

9. Senior management should clearly articulate in the credit institution's policies the roles, responsibilities and authority to act, as well as succession plans. During a disruption, senior management may also need to

   (a) re-align priorities and resources in order to expedite recovery and respond decisively;

   (b) establish a locus of responsibility for managing business continuity, such as a crisis management team with appropriate senior management membership; and

   (c) involve in communicating the institution's response, commensurate with the severity of the disruption.

10. The board and senior management should ensure the implementation of a framework for reporting to them matters related to business continuity, including implementation status, incident reports, testing results and related action plans for strengthening a credit institution's resilience or ability to recover specific operations. They should also ensure that an independent party, such as internal or external auditor, reviews the credit institution's BCM and brings to their attention significant findings on a timely basis.

Risk Identification and Assessment

11. Major operational disruptions pose a substantial risk to the continued operation of credit institutions and to the operation of the financial system. All credit institutions should therefore identify probable disruption scenarios that may lead to short, medium and long-term disruptions to critical business

functions (including outsourced functions) and assess the likelihood of these scenarios occurring.

12. On the basis of practical experiences and potential circumstances and events, credit institutions should develop realistic threat scenarios that may potentially disrupt their business processes and ability to meet their customers' expectations. While threats may include malicious activity[6] as well as natural[7] and technical disasters[8], credit institutions should analyze a threat by focusing on its impact on the credit institution instead of the nature of the threat. For example, by treating the key challenge of an outbreak of disease (e.g. influenza pandemic) as the possibility for low staff availability, which would potentially disrupt business operations for prolonged periods. Likewise, the effects of certain threat scenarios may also be reduced to business disruptions that affect specific work areas, systems, facilities, or geographic locations.

13. The threat scenarios developed by credit institutions need to consider the impact of a disruption and probability of the threat occurring. For example, there may be threats with a high probability of occurrence and low impact to the credit institution (e.g. brief power interruptions). There may also be threats with a low probability of occurrence and high impact on the institution (e.g. terrorism). High probability threats should be supported by very specific BCPs.

14. When assessing the probability of a specific event occurring, credit institutions should consider the geographic location of facilities and their susceptibility to natural threats (e.g., location in a flood area), and the proximity to critical infrastructures (e.g. power plants, airport, highways etc.).

15. The risk assessment should include all the credit institution or service provider's locations and facilities. Worst-case scenarios, such as destruction of the facilities and loss of staff, should be considered. At the conclusion of risk assessment, a credit institution will have estimated how it may be disrupted under various threat scenarios.

16. The extent to which a credit institution prepares to recover from a major operational disruption should be based on its unique characteristics and risk

---

[6] Examples of malicious activities threats include: (i) fraud, theft or blackmail; (ii) sabotage; and (iii) terrorism.

[7] Examples of natural disasters threats include: (i) outbreak of infectious diseases; (ii) fire; (iii) flood and other water damage; (iv) severe weather; (v) air contaminants; and (vi) hazardous chemical spill.

[8] Examples of technical disasters threats include: (i) communications failure; (ii) power failure; (iii) equipment and software failure; and (iv) transportation system disruptions.

profile. Because access to the resources needed for the full recovery of its operations may be limited during a major operational disruption, a credit institution should identify through a business impact analysis those business functions and operations that are to be recovered on a priority basis and establish appropriate recovery objectives for those operations.

Business Impact Analysis

17. A business impact analysis involves identifying all critical business functions (including outsourced functions), resources and infrastructure of the credit institution and assessing the impact of disruption on these functions. The analysis should cover all business units including overseas offices in the case of locally incorporated credit institutions. The factors to be considered in determining the potential financial, legal, reputational and other material consequences if the critical business functions, resources and infrastructure are unavailable include but not limited to:

    (a) the extent to which the interests of customers (including depositors) may be adversely impacted by the disruption to normal services and operations;

    (b) the financial and reputational impact of the failure of the credit institution to perform over a given period of time;

    (c) the revenue loss as a percentage of total revenue;

    (d) the degree of difficulty, including the time taken, in restoring the business activity or support function or implementing alternative arrangements; and

    (e) the ability of the credit institution to meet regulatory requirements if there were business continuity problems.

18. Staff members responsible for carrying out business impact analysis should consider developing uniform interview and inventory questions that can be used on an institutional-wide basis. This can improve the consistency of responses and help to compare and evaluate business process requirements. The business impact analysis process may initially prioritize business processes based on their importance to the institution's achievement of strategic goals and maintenance of safe and sound practices. When determining the credit institution's critical needs, reviews should be conducted for all functions, processes, and personnel within each department / business unit. Each department / business unit should document the mission critical functions performed and consider, for example, the following questions:

    (a) what specialized equipment is required and how is it used?

    (b) how would the department function if mainframe, network and/or Internet access were not available?

(c) what single points of failure exist and how significant are those risks?

(d) what are the critical outsourced relationships and dependencies?

(e) what is the minimum number of staff and space that would be required at a recovery site[9] (see also Appendix 1 for the general requirements of a usable recovery site)?

(f) what special forms or supplies would be needed at a recovery site?

(g) what communication devices would be needed at a recovery site?

(h) what critical operational or security controls require implementation prior to recovery?

(i) is there any potential impact from common recovery sites serving multiple lines of business or departments?

(j) have staff members received cross training and has the department defined back-up functions/roles staff members should perform if key personnel are not available?

19. Based on the results of business impact analysis, a credit institution should be able to identify business functions that are critical and the potential losses should its operations be disrupted. The process also serves to highlight the relative priorities among the various critical functions, estimate how quickly the critical functions can be resumed and help the credit institution determine its recovery strategy.

Recovery Strategy

20. Credit institutions should, based on the results of business impact analysis, establish their recovery strategies that set out recovery objectives and priorities. Among other things, the recovery strategies should indicate the level of services that credit institutions target to provide at various stages during and after operational disruptions as well as the frameworks for ultimately resuming business operations.

21. Individual business and support functions of a credit institution are expected to formulate their own recovery strategies on how to achieve the recovery of a minimum level of critical services within a specified time-frame. This involves the determination of a recovery site, total number of recovery personnel and the related workspace, applications and technology requirements, office facilities and vital records required for the provision of

9 For the purpose of this guideline, a recovery site (or alternative site) is a site ready for use during a business discontinuity event to maintain a credit institution's business continuity. The term applies to both a work space or technology requirements. Appendix 1 gives illustrations on the general requirements of a usable recovery site.

such levels of services. Such strategies are subject to approval by senior management who should also ensure sufficient budget and other resources are allocated on the agreed strategies.

22. In formulating a recovery strategy, credit institutions should assess the interdependency among their own critical services as this would form the basis for determining the recovery priority of individual services and operations. Credit institutions should also take into account the interdependency nature of the financial system and develop recovery objectives that are proportionate to the risk they pose to the operation of the financial system. For example, for those credit institutions that are depended on by other institutions to fulfil the latter institutions' obligations, they are expected to maintain a higher state of business continuity preparedness and to target for highest recovery objectives. For other credit institutions, it may however be acceptable for them to target a less stringent recovery time.

Business Continuity Planning

23. After conducting the risk assessment and business impact analysis and after formulating the recovery strategy, a credit institution should prepare its written BCPs. BCPs are the documented procedures and information which enable the credit institution to respond to a disruption, recover and resume critical business functions. Typically, a BCP establishes the rules and allocates responsibilities for managing operational disruptions and provides clear guidance regarding the succession of authority in the event of a disruption that disables key personnel. A BCP should also clearly set out the decision making authority and define the triggers for invoking the BCP.

24. The business continuity planning process should include all business units and cover all critical business functions, resources and infrastructure, including overseas operations of a Macao incorporated credit institution, and it should also cover arrangements with critical service providers. At a minimum, a BCP should contain:

    (a) the procedures to be followed in response to a material disruption to normal business operations. The procedures should enable the credit institution to manage the initial business disruption, recover and resume the critical business functions, resources and infrastructure outlined in the BCP within the nominated timeframe;

    (b) a list of all resources needed to run operations in the event the primary operational site is unavailable. This would include, but not limited to, computer hardware and software, printers, faxes, telephones, standard stationery and forms. Additional resources include suitable trained staff and relevant documentation such as insurance policies and contracts;

(c) a communication plan for notifying key internal and external parties if the credit institution's BCP is invoked.

(d) consideration of business continuity as part of any material outsourcing agreement with a critical third party service provider (see also the AMCM's Guideline on Outsourcing for additional requirements regarding outsourcing arrangements); and

(e) relevant information about a credit institution's recovery site for the recovery of business and/or IT operations if this forms part of the credit institution's BCP.

25. A consistent method of documenting the BCP should be implemented throughout the credit institution. Detailed input into the BCP should occur at the business unit level. Off-site copies of the BCP should be kept by a number of responsible managers who have designated responsibilities in terms of the BCP and should also be available at the recovery site if applicable.

Communications

26. The ability to communicate effectively with relevant internal and external parties in the event of a major operational disruption is essential for credit institutions. Credit institutions' BCPs should outline internal and external communication channels - with staff, regulators, investors, customers, counterparties, business partners, service providers, the media and other stakeholders. The BCP should also incorporate comprehensive emergency communication protocols and procedures in the case of a major operational disruption. Due to the increasing interdependency and interconnectedness among financial institutions within and across jurisdictions, credit institutions' BCPs should contain communication protocols for contacting relevant non-domestic financial authorities and institutions in different jurisdictions.

27. The communication procedures of credit institutions generally should:

(a) identify those responsible for communicating with staff and various external stakeholders. This group might include senior management, public affairs staff, legal and compliance advisors, and staff responsible for the credit institution's business continuity procedures;

(b) build on any communication protocols that already exist within the financial system and include contact information for the AMCM and other credit institutions to facilitate an assessment of the condition of the financial system and coordinate recovery efforts;

(c) address related issues that can arise during a major operational disruption, such as how to respond to failures in primary communication systems. This could include, for example, developing systems and contact information for key personnel that would facilitate multiple methods of communicating (e.g. pagers, mobile phones, email or two-way radios, etc); and

(d) provide for the regular updating of calling trees and other contact information and the periodic testing of calling trees.

Testing

28. Credit institutions should test their BCPs, evaluate their effectiveness and update their BCPs as appropriate. In light of the possible changes in technology, business processes and staff members' roles and responsibilities, continuous reviews and meaningful testing of all components of the BCP should be undertaken to reflect the risks and the changing circumstances faced by the credit institution, to familiarize staff members with the operation of the BCP, to verify that the BCP is practically workable, and to identify issues which need to be addressed but which were not apparent during the planning stage.

29. The conditions and frequency for testing should be detailed in a testing strategy, which should include test objectives, scripts, and schedules, as well as provide for review and reporting of test results. Testing should be conducted at least annually depending on the operating environment and criticality of the relevant applications and business functions. Where appropriate, credit institutions should also participate in industry-wide test exercises conducted by industry association(s) (e.g. the Macao Association of Banks). These efforts will help credit institutions raise their state of readiness as well as the resilience of the financial system to cope with major operational disruptions.

30. Ideally, testing should be undertaken by the team who will operate the BCP to ensure effective team working, preparedness and awareness. It is also advisable to rotate personnel involved in testing in order to prepare for the loss of key individuals, both during a disruption and as a result of retirements, promotions, terminations, resignations, or re-assignment of responsibilities.

31. Testing methods vary from minimum preparation and resources to the most complex. The type of testing employed by a credit institution should be determined by, among other things, its size, complexity, and nature of its business. Examples of testing methods in order of increasing complexity include:

(a) an orientation/walk-through. The primary objective of the walk-through is to ensure that critical personnel from all areas are familiar with the BCP. It is characterized by:

- discussion about the BCP in a conference room or small group setting;
- individual and team training; and
- clarification and highlighting of critical plan elements.

(b) a tabletop/mini-drill. In such a drill, the participants choose a specific event scenario and apply the BCP to it. It includes:

- practice and validation of specific functional response capability;
- focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability;
- role playing with simulated response at recovery sites/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment;
- mobilization of all or some of the crisis management/response team to practise proper coordination; and
- varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.

(c) functional testing. It involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the BCP. It includes:

- demonstration of emergency management capabilities of several groups practising a series of interactive functions, such as direction, control, assessment, operations, and planning;
- actual or simulated response to recovery sites or facilities using actual communications capabilities;
- mobilization of personnel and resources at varied geographical sites; and
- varying degrees of actual, as opposed to simulated, notification and resource mobilization.

(d) full-scale testing. In a full-scale test, the credit institution implements all or portions of its BCP by processing data and transactions using back-up media at the recovery site. It involves:

- validation of crisis response functions;
- demonstration of knowledge and skills, as well as management response and decision-making capability;

- on-the-scene execution of coordination and decision-making roles;
- actual, as opposed to simulated, notifications, mobilization of resources, and communication of decisions;
- activities conducted at actual response locations or facilities;
- institutional-wide participation and interaction of internal and external management response teams with full involvement of external organizations;
- actual processing of data utilizing back-up media; and
- exercises generally extending over a longer period of time to allow issues to fully evolve as they would in a crisis, and allow realistic role-play of all the involved groups.

32. Test results should be analyzed and compared against stated objectives. Test results and the resolution of any problems should be reported to the board and senior management. The test analyses should include:

(a) an assessment of whether the test objectives were completed;

(b) an assessment of the validity of test data processed;

(c) corrective action plans to address problems encountered;

(d) a description of any gaps between the BCP and actual test results;

(e) proposed modifications to the BCP; and

(f) recommendations for future tests.

Training and Awareness

33. Credit institutions should provide business continuity training for their management and staff to ensure all parties, especially members of the business continuity team, are aware of their responsibilities should a disruption occur. Key staff members of credit institutions should be involved in the business continuity development process, as well as periodic training exercises. The training program should incorporate institutional-wide training as well as specific training for individual business units. Staff members of credit institutions should be aware of:

(a) the importance of BCM within the credit institution's overall risk management framework;

(b) the conditions call for implementing all or parts of the credit institution's BCP;

(c) the person(s) who is responsible for implementing BCPs for business units and the credit institution and his/her emergency contacts; and

(d) what to do if the key staff members are not available at the time of a disruption.

Cross training should be utilized to anticipate restoring operations in the absence of key staff members. Staff training should be regularly scheduled and updated to address changes to the BCP.

34. Credit institutions should consider developing an awareness program to let customers, service providers, and regulators know how to contact them if normal communication channels are not in operation. The plan should also designate personnel who will communicate with the media, government, vendors, and other entities and provide for the type of information to be communicated.

Crisis Management

35. The BCP should set out a crisis management process that serves as documented guidance to assist credit institutions in identifying potential crisis scenarios and develop procedures for managing these scenarios. Credit institutions should establish crisis management teams, comprised of senior management and heads of major support functions, to respond to and manage the various stages of a crisis.

Updating BCP

36. The BCP should be reviewed by senior management, the planning team or coordinator, team members, internal audit, and the board at least annually. As part of that review process, the team, or coordinator should contact business unit managers throughout the credit institution at regular intervals to assess the nature and scope of any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities.

Audit and Independent Reviews

37. The audit department or other qualified, independent party should review the adequacy of the business continuity process to ensure the board's expectations are met. This review should include, for example, assessing the adequacy of business process identification, risk assessments, threat scenario development, business impact analysis, the BCP, testing scenarios and schedules, and communication of test results and recommendations to the board etc. In order to discharge these responsibilities, the audit department or other independent party should directly observe tests of the BCP. The board should receive and carefully review audit reports on the effectiveness of the institution's process

that identify any areas of weakness.

Insurance Consideration

38. Insurance is commonly used to recoup losses from risks that cannot be completely prevented. In addition to the above BCM processes, credit institutions should also consider obtaining insurance coverage for those risks that cannot be entirely controlled but which could represent a significant potential for financial loss or other disastrous consequences. For example, insurance coverage for the loss of staff, offices, and critical IT facilities / equipment as well as insurance coverage to address the credit institutions' legal responsibilities for failing to deliver services to their customers etc. The decision to obtain insurance should be based on the probability and degree of loss identified during the business impact analysis. The potential exposure for various types of disruptions should be determined and the insurance options available should be reviewed to ensure appropriate insurance coverage is provided. Credit institutions should perform an annual insurance review to ensure the level and types of coverage are commercially reasonable and consistent with any legal, management, and board requirements. They should also create and maintain a comprehensive hardware and software inventory list in a secure off-site location in order to facilitate the claims process. Credit institutions should nevertheless be aware of the limitations of insurance, which is by no means a substitute for an effective BCP and which cannot reimburse a credit institution for damage to its reputation.

AMCM's Supervisory Approach

39. The AMCM expects credit institutions to develop and implement effective BCM that is consistent with the above-mentioned principles and key processes. Credit institutions should also update their BCPs on an ongoing basis.

40. The AMCM would incorporate BCM reviews into its frameworks for the assessment of credit institutions. Assessments would give due consideration to whether a credit institution's BCM, including its recovery objectives, is appropriate for the size and scope of its business and the risk the credit institution presents to the continued operation of the financial system.

41. The AMCM would also assess whether credit institutions are taking appropriate steps to augment their BCM, where necessary.

42. In the course of reviewing a credit institution's BCM, the AMCM would assess whether the testing programme provides adequate assurance that business processes can be recovered as intended.

Appendix 1

General Requirements of a Usable Recovery Site for Business Continuity Purpose

1. It can be either an external site available through an agreement with a third party or a site owned by the credit institution.

2. It should be sufficiently distanced to avoid being affected by the same disruption as the primary site.

3. It should be readily accessible and available for occupancy within the time requirement specified in the BCP.

4. It should be adequately equipped with the necessary workstations, power, telephone and ventilation, and has sufficient space.

5. Appropriate physical access controls should be implemented in the site in accordance with the credit institution's security policy.

6. Sufficient technical equipment of appropriate model, size and capacity should be available in the site to meet recovery requirements as set out in the BCP.

7. Adequate telecommunication facilities and pre-installed network connections should be available to handle the expected volume of business as specified by the BCP.

8. Continuous monitoring and periodic maintenance and testing of equipment and facilities should be conducted to keep the site operational.

9. Vital records should be readily accessible at the site for emergency retrieval by staff members.