Monetary Authority of Singapore

BUSINESS CONTINUITY MANAGEMENT GUIDELINES

June 2003

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 READINESS IS YOUR ONLY PROTECTION[1]

1.1.1 The global financial system is a set of interlinked networks of markets, systems, and participants. While financial institutions ("institutions")[2] acknowledge the need to strengthen their resilience against disruptions, they also recognise that the network is only as strong as its weakest link and the potential impact of a major operational disruption may incapacitate the financial system.

1.1.2 The quick recovery[3] of business functions after disruption is therefore crucial in maintaining confidence in institutions. Failing which, institutions may compromise its business obligations, which may result in significant financial losses and potentially lead to a contagion effect on the financial system. Insurance coverage may compensate certain quantifiable losses but would not protect institutions against the erosion of brand value or the loss of customers' confidence.

1.1.3 Business Continuity Management ("BCM") is an over-arching framework[4] that aims to minimise the impact to businesses due to operational disruptions. It not only addresses the restoration of information technology ("IT") infrastructure, but also focuses on the rapid recovery and resumption of critical business functions for the fulfilment of business obligations. One important tangible evidence that the institutions have embraced BCM is the formulation of a business continuity plan ("BCP").

1.1.4 Increasingly, globalisation and technological advancements are constantly testing the boundaries of implementing an effective BCM. A key challenge for institutions is to establish and maintain a comprehensive BCM that is cost-effective without a compromise of prudent risk management policies and fulfil its business obligations during a disruption. This is a continuous process. As changes in technology, business focus, and staff affect the state of

[1] Slogan of Singapore's Civil Defence.
[2] Includes regulated financial institutions and financial utility providers. Financial utility providers are organisations that provide specialised financial services such as cheque clearing and settlement.
[3] The course of action for rebuilding functions to the condition where they are ready to process data or information. This condition should be at a level sufficient to meet outstanding business obligations.
[4] A framework that includes policies, standards, and procedures that provides for continuous functioning of the institution during operational disruptions. It is commensurate with the institutions' nature, scale, complexity of business activities.

preparedness, increasingly, institutions recognise the need to incorporate BCM as an ongoing discipline into its business-as-usual operations and thereby improve its readiness to respond to and recover from crises.

1.1.5 Management prudence is therefore important in this continuous process.

1.2 APPLICATION OF THE GUIDELINES

1.2.1 The guidelines are sound BCM principles and serve as standards that institutions are encouraged to adopt. Institutions may adapt the guidelines as necessary, taking into account the diverse activities they engage in and the different markets in which they conduct transactions. Ultimately, the responsibility for business continuity preparedness and recovery following operational disruptions rests with institutions. MAS will endeavour to update the guidelines in response to international developments as they evolve.

1.2.2 One of MAS' key supervisory objectives is for institutions to have continuity plans in place to allow the continuation of critical business operations and fulfilment of business obligations in the event of disruptions. Institutions are encouraged to implement and maintain BCM that is commensurate with the institutions' nature, scale, and complexity of business activities.

1.2.3 BCM remains an important contributing factor in MAS' overall supervisory assessment. MAS will, in the course of its supervision of institutions, review the BCP implemented, taking into consideration the extent to which the institution observed the guidelines, and its risk profile. Institutions are encouraged to accept and adopt the sound principles, and develop implementation plans taking into consideration their business activities and operating environment.

1.2.4 Due to the interdependent nature of the financial system, institutions may have differing recovery expectations of each other and of the industry. Some institutions are expected to maintain a higher state of business continuity preparedness because of the extent to which other institutions depend on them to fulfil their obligations. A few of these institutions are depended on by the financial industry, to the degree that their failure to recover from operational disruption may contribute towards the amplification of systemic risk. For the purpose of these guidelines, they are collectively referred to as Significantly Important Institutions ("SII"). The financial sector would expect SII to be better prepared and aligned closer to the guidelines. MAS will, in the course of its supervision, be in contact with those institutions considered by MAS to be SII, and will discuss with them MAS' expectations regarding adherence to the guidelines.

1.2.5 Senior management and BCM practitioners should familiarise themselves with the guidelines and understand the intent and implications of the sound principles. Institutions should also read the guidelines in conjunction with relevant regulatory requirements and industry standards.

Institutions are encouraged to conduct a self-assessment of their business continuity preparedness against these sound principles and bring deficiencies to their senior management's attention as soon as possible.

1.3 GLOSSARY

Terminology	Definitions (as used in this document)
BCM	Business Continuity Management. Refers to an over-arching framework that includes policies, standards, and procedures that provides for continuous functioning of the institution during operational disruptions. It is commensurate with the institutions' nature, scale and complexity of business activities.
BCP	Business Continuity Plan. A plan of action that sets out the procedures and establishes the processes and systems necessary to restore the orderly and expeditious operation of the institution in the event of disruptions to the operations of the institution.
BIA	Business Impact Analysis. The process of measuring the business impact or loss (quantitatively and qualitatively) to the institution in an outage. The BIA is useful in identifying the recovery priorities, recovery resources requirements, recovery strategies, and critical staff.
Business Recovery	The course of action for rebuilding functions to the condition where they are ready to process data or information. This condition should be at a level sufficient to meet outstanding business obligations.
Business Resumption	The condition of a function, following its recovery, when it is ready to take on tasks and activities to meet new business obligations.
Recovery Strategies	Defined, management-approved and tested course of action in response to operational disruptions.
Recovery Time Objective	Target duration of time to recover a specific business function. It comprises two components: (1) The duration of time from the point of disruption, to the point of declaring the activation of BCP, and (2) The duration of time from the activation of the BCP to the point when the specific business function is recovered. (Refer to business recovery) It is the acceptable duration of time that can elapse before the non-continuation of the specific business function would result in severe business impact and losses to the institution.
Residual Risk	Risk that remain after mitigating measures have been applied.
Systemic Risk	Includes the risk that the failure of one institution in the financial system to meet its required obligations will cause other institutions to be unable to meet their obligations when due, thereby potentially causing significant liquidity dislocations or credit problems and threatening the stability of the financial markets.

2.0 BUSINESS CONTINUITY MANAGEMENT PRINCIPLES

2.1 PRINCIPLE 1: BOARD OF DIRECTORS AND SENIOR MANAGEMENT SHOULD BE RESPONSIBLE FOR THEIR INSTITUTION'S BUSINESS CONTINUITY MANAGEMENT.

2.1.1 The responsibility for the state of business continuity preparedness of an institution ultimately lies with the Board of directors and senior management.

2.1.2 Senior management is responsible for steering BCM with policies and strategies necessary for the continuation of critical business functions. In addition, they should demonstrate that they have sufficient awareness of the risks, mitigating measures and state of readiness by way of an attestation to the Board of directors.

2.1.3 The attestation is an internal document addressed to the Board of directors[5] for their endorsement. Senior management should determine the form that best provides them the level of comfort and the need for further assurance. The attestation should state clearly the:

- Preparedness of the institution and
- Extent of alignment with the guidelines that is commensurate with the institution's nature, scale and complexity of business activities

MAS also encourages the disclosure and inclusion of residual risk[6] in the attestation.

2.1.4 The attestation should be updated at least once a year or more frequently should there be material change within the institution.

2.1.5 While some customers and counterparties may look to institutions that they have financial dealings with for assurance on their business continuity preparedness, institutions are responsible for determining and decide on the necessary disclosure of the attestation to customers and counterparties.

[5] For overseas incorporated institutions in Singapore, the attestation should be addressed to the relevant function responsible for BCM at Group/Global level.
[6] Risk that remains after mitigating measures have been applied.

2.2 PRINCIPLE 2: INSTITUTIONS SHOULD EMBED BUSINESS CONTINUITY MANAGEMENT INTO THEIR BUSINESS-AS-USUAL OPERATIONS, INCORPORATING SOUND PRACTICES.

2.2.1 BCM is a risk-based framework that addresses operational risk by developing clear policies, strategies, and accountabilities for the recovery of critical business functions. It is a proactive process. Institutions should therefore strive to build an organisational culture that embed BCM as part of their business-as-usual operations and day-to-day risk management.

2.2.2 Depending on the scale and complexity of the businesses, institutions could adopt sound BCM practices[7] that include the following components:

- Clear BCM policy, strategy and budget
- Well-defined roles and responsibilities for the BCM programme
- BCP comprising of detailed tasks and activities
- Succession plans for critical staff and senior management
- Business impact analysis or similar process
- Programme for the development, implementation, testing and maintenance of BCP
- Programmes for training and awareness
- Emergency responses
- External communications and crisis management coordination programmes
- Coordination with external parties (including authorities, interdependent parties, etc.)

2.2.3 The BCP is an important, tangible evidence of an institution's BCM initiative. It should be practical in operation, regularly reviewed, updated as the business changes, and meaningfully tested to ensure its relevancy, effectiveness, and operational viability.

[7] In developing the BCM framework, institutions may want to consider drawing additional references from BCM organisations such as The Disaster Recovery Institute International (www.drii.org) or The Business Continuity Institute (www.thebci.org).

2.3 PRINCIPLE 3: INSTITUTIONS SHOULD TEST THEIR BUSINESS CONTINUITY PLAN REGULARLY, COMPLETELY, AND MEANINGFULLY.

2.3.1 Testing[8] is a vital element for implementing an effective BCM. Changes in technology, business processes and staffs' roles and responsibilities can affect the appropriateness of the BCP; and ultimately the business continuity preparedness of institutions. It is therefore important to regularly test its functionality and effectiveness. Tests will also familiarise staff with the location of the recovery site, as well as the recovery procedures. Institutions should seek assurance from testing, that should they activate their BCP, they would be able to continue to operate reliably, responsively, and efficiently as planned.

2.3.2 **Regular:** Institutions are encouraged to carry out different types of tests. Taking into consideration the criticality of the business functions, the complexities and resources required, institutions could conduct tests in modules and at different but regular intervals. Senior management and staff should participate in these exercises and be familiar with their roles and responsibilities in the event of activation.

2.3.3 **Complete and meaningful:** All components of a business process should be meaningfully tested (e.g. from front-line through to supporting and processing components, etc.). This should include testing the connectivity, functionality and load capacity of the infrastructure provided at the recovery site(s). Institutions should satisfy themselves that their exercise programmes adequately cover both the qualitative (e.g. response time, etc.) and quantitative (e.g. volume capacity, etc.) aspects. They should critically challenge all strategic and planning assumptions regularly to ascertain their applicability, especially when business scope or direction changes. Completeness would also include the awareness and preparedness of staff and coordination with external parties, as well as thorough testing of all interdependencies. This would include the institutions' offices, branches or service providers based outside Singapore.

2.3.4 Institution-wide tests are also encouraged as it offers a different perspective from that of modular tests. Institutions should progressively make their exercises more challenging and introduce different scenarios each time they conduct the same type of exercise. This would lead to an increase in confidence of their business continuity preparedness. Exercises may include:

[8] Testing encompasses exercises, rehearsals, etc. In this document, the words 'test' and 'exercise' are used interchangeably.

- Desk-top walk-through exercise to full system test
- Staff call-tree activation (with and without mobilisation)
- Back-up site to back-up site exercise (including with external service providers)
- Alternative arrangements of shared services
- Back-up tape restoration and
- Retrieval of vital records

Ultimately, institutions have to satisfy themselves that such tests and exercises contribute meaningfully towards enhancing their business continuity preparedness.

2.3.5 Formal exercise documentation and post mortem reviews listing lessons learnt and any new risk mitigating measures should be prepared. Senior management should sign-off on the documentation and concur with the proposed new mitigating measures.

2.3.6 **Industry-wide:** Appropriately scaled and coordinated exercises between key financial utility providers[9] and the institutions they service would increase the level of awareness and confidence in recovery operations. It would also serve to increase the confidence in the financial sector network. Institutions with such dependencies should participate in these exercises.

[9] Financial utility providers are organisations that provide specialised financial services such as cheque clearing and settlement.

2.4 PRINCIPLE 4: INSTITUTIONS SHOULD DEVELOP RECOVERY STRATEGIES AND SET RECOVERY TIME OBJECTIVES FOR CRITICAL BUSINESS FUNCTIONS.

2.4.1 The establishment of recovery strategies enables institutions to execute their BCP in an orderly and predefined manner that minimises disruption and financial loss. Recovery strategies form the basis for defining recovery time objectives[10] of critical business functions. Without these clear markers, scarce resources may be inappropriately diverted to less important activities. This may adversely affect the institutions' reputation and survivability.

Critical business functions

2.4.2 In a crisis, it might not be practical to recover all business functions at the same time. Institutions should therefore identify business functions that are critical (including support operations and related IT systems) and the potential losses (in monetary and non-monetary terms) should their operations be disrupted. A common process used to obtain this information is a business impact analysis ("BIA")[11]. This process also serves to highlight the relative priorities among the various critical functions and help institutions determine their recovery strategies and recovery time objectives.

2.4.3 Critical business functions differ among institutions largely due to different business focus and customers' expectations. Some critical business functions would include; completing payment instructions, clearing and settling transactions, fulfilling end-of-day funding and collateral obligations, managing customers' risk positions and maintaining customer, investor or public confidence.

Recovery time objectives

2.4.4 Recovery time objectives may range from minutes to hours. For some industry sectors and functions, it could be longer. For the reasons stated earlier, it is important for SII to recover and resume their critical business functions faster than the institutions or the industry that depend on them.

2.4.5 The transparency and sharing of recovery time objectives would help improve service level expectations and understanding among institutions and further contribute towards the mitigation of interdependency risk.

[10] Refer glossary.

[11] The process of measuring the business impact or loss (quantitatively and qualitatively) to the institution of an outage. The BIA is useful in identifying the recovery priorities, recovery resources requirements, recovery strategies, and critical staff.

Determining recovery time objectives for critical business functions

2.4.6 Institutions are responsible for determining their critical business functions, recovery strategies and the corresponding recovery time objectives that is commensurate with the nature, scale and complexity of their business functions and business obligations.

2.4.7 It is unlikely that all critical business functions would share the same recovery time objective. There should be a continuum of recovery time objectives for different business functions that is commensurate with institutions' obligations to the market, customers and industry.

2.5 PRINCIPLE 5: INSTITUTIONS SHOULD UNDERSTAND AND APPROPRIATELY MITIGATE INTERDEPENDENCY RISK OF CRITICAL BUSINESS FUNCTIONS.

2.5.1 Increasingly, there is a tendency for institutions to slice and redistribute risk and processes locally, regionally or globally, leading to increased dependency on either internal or external parties. Any mismanagement of these dependencies and the risks they entail could cascade into operational or systemic inefficiencies, potentially leading to the failure of institutions.

2.5.2 When planning for the business continuity of critical business functions, institutions should take into account the interdependencies of these business functions, and the extent to which they depend on other parties. Institutions should also understand the business processes of these parties that support their critical functions, including their business continuity preparedness and recovery priorities.

Examples of such dependencies are:

- Within an institution (e.g. Treasury, custody services, etc.)
- Between institutions (e.g. for US Dollar clearing, etc.)
- On financial utility providers (e.g. clearing and settlement providers, etc.)
- On vendors (e.g. IT or disaster recovery service providers, etc.)
- On infrastructure providers (e.g. telecommunication, etc.)

2.5.3 Institutions should mitigate the risk arising from these complex dependencies as far as practically possible and consider such dependencies in their recovery strategies and recovery time objectives. For example, institutions with customers, counterparties, or service providers whose primary sites are also within the same zone[12] could arrange telecommunication links between their recovery sites and test them regularly.

2.5.4 Although some of the interdependency risks are beyond the institutions' direct control to mitigate completely (e.g. unavailability of telecommunication networks, etc.), this may not dilute their customers' and counterparties' expectation of the institutions' services and obligations. It is the responsibility of institutions to take reasonable steps (e.g. initiate discussions with telecommunications provider on redundancy capabilities, etc.) to ensure that

[12] Please refer to principle 6 for an understanding of what represents a zone.

their key service providers are capable of supporting their businesses, even in disruptions. Institutions could consider engaging common service providers in BCM discussions through their respective industry associations.

2.5.5 Before contracting with external service providers, institutions should satisfy themselves that the risk resulting from outsourcing remains within levels permitted by their operational risk management policies and does not compromise business continuity preparedness. They should ensure that their service providers have BCP in place that is equal to, if not more robust than, their own. Institutions should proactively seek assurances that their service providers' BCP are regularly tested.

2.5.6 Following the appointment of external service providers, it is vital that institutions continue to monitor their financial well-being and gather market intelligence to discern early warning signs of potential problems.

2.5.7 In addition, institutions should mitigate the risk of unexpected termination or liquidation of key service providers that their critical business functions depend on. This is because institutions may take many months to implement an alternative solution. To this end, institutions should take reasonable steps to retain an appropriate level of control and reserve the right to intervene with appropriate measures to continue their critical business operations.

2.5.8 Ultimately, the risk of interdependency lies with the institutions and cannot be 'assumed' away. Institutions are responsible for balancing the risk and cost trade-offs, address the risk adequately and take reasonable steps that are commensurate with the criticality of the business function as well as the size and nature of operations.

2.6 PRINCIPLE 6: INSTITUTIONS SHOULD PLAN FOR WIDE-AREA DISRUPTIONS.

2.6.1 The 11 September 2001 incident demonstrated that institutions should plan for disruptions that affect a wide-area ("zone"). Due to a number of factors such as the differing size and complexity of business operations across all institutions in Singapore, it would not be appropriate nor practical, to standardise on a criteria that defines a zone that could be applied equally across the financial sector.

2.6.2 MAS looks to institutions to demonstrate that they have planned and catered for a wide-area disruption in their BCM. Some planning parameters that institutions may consider are; the geographical concentration of institutions, transactional processing activities, and dependencies on internal or external service providers.

2.6.3 Depending on the operational set-up of institutions, wide-area disruptions may heighten interdependency risk between critical functions and service providers within the same zone. This could be due to widespread disruption of critical services such as telecommunications failure or the inaccessibility of critical staff. Such risk should be mitigated appropriately.

2.6.4 Institutions are responsible for deciding on the need to cater for multiple zones outage scenarios, taking into consideration their respective levels of critical business activities and prudent risk management policies. In addition, they should also consider broadening and deepening their BCM scope to cater for prolonged operational disruptions.

2.7 PRINCIPLE 7: INSTITUTIONS SHOULD PRACTISE A SEPARATION POLICY TO MITIGATE CONCENTRATION RISK OF CRITICAL BUSINESS FUNCTIONS.

2.7.1 There are economic benefits to the centralisation of critical business and support functions such as treasury front and back-office as well as IT data centre. However, institutions risk losing their ability to recover these functions in a disruption, should there be a significant loss of staff or technology.

2.7.2 Critical staff and information are important assets that are difficult to replace quickly. Many institutions assume that the same pool of staff would be available to recover their critical business functions at the recovery sites. This may not always be true as disruptions may result in the unavailability of critical staff. Also, identifying alternates to critical staff may not always reduce the risk, especially if both the primary and alternate critical staff are housed in the same location or zone.

2.7.3 It is important therefore, to find the right balance between mitigating concentration risk and not losing the efficiencies gained from the centralisation of business processes and critical staff. To mitigate concentration risk of critical business functions, institutions could consider the following approaches:

2.7.4 **Primary-secondary site separation.** Separate the primary and secondary sites of critical business functions into different zones. This would mitigate the risk of losing both sites in a wide-area disruption.

2.7.5 **Critical business functions separation and intra-function separation.** Separating critical business functions into different zones would mitigate the risk of losing multiple critical business functions from a single-zone disruption. Similarly, diversifying critical business functions (eg. back-office settlement operations and critical IT support, etc.), such that another labour pool in a different zone is able to take over these functions during disruptions, would eliminate the dependency on a single labour pool.

2.7.6 These approaches have different cost implications. While cost is an important consideration, institutions should design and determine the most appropriate approach, or combination of approaches that best balances cost and risk exposure that provides an adequate level of comfort and assurance. The mitigating solution should be commensurate with the nature, scale, and complexity of their business functions.

2.7.7 Institutions are encouraged to be innovative and explore different avenues of mitigating concentration risk.