



The Monetary Authority of Singapore

MAS Consultation Paper

**GUIDELINES ON
BUSINESS CONTINUITY
PLANNING**

10 January 2003

INVITATION TO COMMENT

The Monetary Authority of Singapore (“MAS”) invites comment from financial sector participants and interested parties on the proposed guidelines. Your comments will help MAS develop practical supervisory response to the challenges facing the financial sector concerning business continuity planning.

Please submit your responses to MAS no later than 10 February 2003. An early response would be appreciated.

Please send your responses to:

Specialist Risk Supervision Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Attention: Industry BCP Officer

Fax: (65) 6229 9659
Email: bcp@mas.gov.sg

Please note that your comments may be made public unless confidentiality is expressly requested.

This consultation paper (“Paper”) is released to financial institutions via MASNET and MAS’ website (<http://www.mas.gov.sg>). Industry associations such as the Association of Banks in Singapore, Life Insurance Association of Singapore and Securities Association of Singapore have also been notified.

TABLE OF CONTENTS

INVITATION TO COMMENT	2
EXECUTIVE SUMMARY	4
SECTION 1 : INTRODUCTION	5
Background.....	5
The need for guidance on business continuity planning.....	5
Application of the principles	6
Purpose of this consultation paper.....	6
SECTION 2 : BUSINESS CONTINUITY PLANNING.....	7
Readiness Is Your Only Protection	7
Supervisory approach	7
Glossary.....	8
SECTION 3 : PRINCIPLES	9
Principle 1: Board and management should take responsibility for the BCP preparedness of their institution.	9
Principle 2: Institutions should embed BCP into their business-as-usual operations, incorporating sound practices.....	9
Principle 3: Institutions should test their BCP regularly, completely and meaningfully.	10
Principle 4: Institutions should develop recovery strategies and set recovery time objectives for critical business functions.	12
Principle 5: Institutions should understand and appropriately mitigate interdependency risks of critical business functions.....	13
Principle 6: Institutions should plan for wide-area (zonal) disruptions.....	14
Principle 7: Institutions should practise separation policy to mitigate concentration risk.....	15
APPENDIX A – SPECIFIC LESSONS FROM SEPTEMBER 11	16

EXECUTIVE SUMMARY

This consultation paper proposes seven principles on business continuity planning (“BCP”)¹ in response to financial institutions’² (“institutions”) requests for guidance. Institutions are encouraged to consider and adopt these principles.

The financial sector is a global network of markets, systems and participants. While institutions acknowledge the need to strengthen their resilience against disruptions and to reduce the probability that wide-scale disruptions may bring the financial sector to a standstill, they also recognise that the financial sector is highly interdependent and is only as strong as its weakest link.

Institution’s Board and management recognise that the implementation of BCP is essential and should be embedded into their business-as-usual operations. However, the challenge is to implement a comprehensive BCP that minimises investments and resources without compromising their risk management policies and business obligations.

The events of 11 September 2001 (“September 11”) have also highlighted vulnerabilities that may not have been fully appreciated before, such as, the concentration of staff, processes and technology.

MAS will, in the course of its supervision of institutions, review the BCP implemented, taking into consideration the institution’s alignment with the principles and their risk profile and role in preserving the systemic stability of the financial system. BCP is an important contributing factor in MAS’ overall supervisory assessment of the institutions.

Questions have been included at the end of each principle to help highlight pertinent issues. MAS seeks comments from financial sector participants and interested parties on the proposed guidelines.

¹ In this document, depending on the context of the sentence, BCP could either mean business continuity plan or business continuity planning. In some instances, it is used as a noun (e.g. BCP issues).

² Includes financial institutions and financial utility providers. Financial utility providers are organisations that provide specialised financial services such as clearing and settlement functions etc.

SECTION 1 : INTRODUCTION

Background

1.1 The quick recovery and resumption of business operations after disruption is critical to minimise impact and maintain confidence in any institution. Failing which, it may result in inability to fulfil critical or all of an institution's business obligations. This can, in turn, result in significant financial losses or even cause contagion or systemic impact with broader disruptions to the financial system. Insurance coverage may recover certain quantifiable losses but would not protect against the erosion of brand value or the loss of customers' confidence in the institution.

1.2 BCP is the development of plans, processes and procedures to minimise the adverse impact on an institution's business. It not only addresses an institution recovering their information technology (IT) infrastructure, it should also focus on the rapid recovery and resumption of critical business functions and the fulfilment of business obligations.

The need for guidance on business continuity planning

1.3 The financial sector is an interdependent global network of markets, systems, and participants. In this context, the financial sector network is only as strong as the weakest link. That institutions acknowledge the need to strengthen their resilience against disruptions and to reduce the probability that wide-scale disruptions may bring the financial sector to a standstill is evident by the number of requests received from institutions for MAS to provide guidance and views on BCP.

1.4 The events of September 11 have highlighted vulnerabilities that may not have been fully appreciated before (refer to Appendix A for more details). It also highlighted the high degree of interdependency within the financial sector and the need to review institutions and regulatory approaches towards BCP. Singapore is not alone in this effort. There is an increasing need internationally for greater coordination of BCP activities between regulators and institutions. Supervisors in many developed jurisdictions and international bodies such as BIS-CPSS³ are currently sharing views on BCP practices and the appropriate way forward. MAS will endeavour to align the principles with these international efforts as they evolve.

1.5 The principles in this Paper are in response to these requests and vulnerabilities identified. They aim to maximise the resilience of institutions and the financial sector. They are not intended to prescribe how institutions should conduct their BCP process.

³ Bank for International Settlements – Committee on Payment and Settlement Systems

Application of the principles

1.6 One of MAS' key supervisory objectives is for institutions to have BCP in place to allow the continuation of critical businesses, fulfil obligations and service-level commitments in the event of disruptions. While institutions are encouraged to adopt these principles, MAS recognises that institutions may adhere to the principles to varying degrees. Significantly important institutions⁴ are expected to align closer to these principles and maintain a higher state of preparedness.

1.7 Senior management and BCP practitioners are expected to read the Paper and understand the intent and implications of the principles for their institutions.

Purpose of this consultation paper

1.8 Section 2 of this Paper gives an overview of the challenges for business continuity planning and supervisory approach. Section 3 details the proposed seven principles. Questions have been included at the end of each principle to help highlight pertinent issues and solicit comments. MAS intends to release the guidelines by March 2003.

⁴ A significantly important institution is defined as one that has a critical role in preserving the systemic stability of the financial system. It would present systemic risk and/or affect public or investor confidence should they be unable to complete (recover) and carry-on (resume) critical functions and activities.

SECTION 2 : BUSINESS CONTINUITY PLANNING

Readiness Is Your Only Protection⁵

2.1 A key challenge for institutions is to establish a comprehensive BCP that minimises investments and resources without compromising their risk management policies and business obligations. This is a continuous process as institutions are not static and changes in technology, business focus, or staff do affect the BCP.

2.2 BCP is a discipline that needs to be weaved into the fabric of the institutions' day-to-day management and operations. Institutions with this culture and mindsets at all levels are better placed to respond to crises.

2.3 Developing BCP should not only be viewed as a cost-benefit and probability assessment exercise. It should also be risk-focussed. It is important that the Board and management demonstrate leadership and assume responsibility for the BCP preparedness of their institution.

Supervisory approach

2.4 Institutions should have in place risk management policies and processes aimed at safeguarding their operational capability in the event of disruptions. Institutions are therefore expected to manage their operational risks posed by such disruptions.

2.5 Resilience is as important as recovery. While the former is preventive in nature, recovery is a reactive process of rapidly restoring the institution to the state operational readiness. All institutions should implement and maintain a risk-focus BCP framework⁶. This should take into account both aspects of resilience and recovery, as well as the nature, scale and complexity of their businesses. Risk mitigating measures should be commensurate with the institutions' level of business activity, risk tolerance and role in preserving the systemic stability of the financial system. Such measures should be clearly documented in the Business Continuity Plan and regularly reviewed, maintained and tested.

2.6 MAS will, in the course of its supervision of institutions, review the BCP implemented, taking into consideration the following factors:

- The extent to which the institution observed the principles, and
- The risk profile of the institution and their role in preserving the systemic stability of the financial system

BCP is an important contributing factor in MAS' overall supervisory assessment.

⁵ Slogan of Singapore's Civil Defence.

⁶ A framework that includes policies, standards and procedures that commensurate with the risk profile of the institution. It sets out the business continuity planning process.

Glossary

<u>Terminology</u>	<u>Definitions (as used in this document)</u>
Business Continuity Planning (BCP)	The pre-emptive planning and preparations that is necessary to identify the impact of potential losses arising from an emergency or a disaster. To develop recovery plans that ensure the continuity of an institution's critical services in that relation. Sometimes used as a noun (e.g. BCP issues).
BCP Framework	A framework that includes policies, standards and procedures that is commensurate with the risk profile of the institution. It sets out the business continuity planning process.
Business Impact Analysis (BIA)	The process of determining the impact (loss) to the institution of an outage by measuring the impact quantitatively and qualitatively, where possible. It would assist management in developing their recovery strategies.
Recovery Strategies	A defined, tested, management-approved course of action to be employed in response to a business disruption, interruption, or disaster.
Recovery Time Objectives	The maximum acceptable length of time that can elapse before the lack of a business function severely impacts the business entity. It comprises of two components: the time before a disaster is declared, and the time to perform tasks to the point of business resumption.
Significantly Important Institutions	A significantly important institution is defined as one that has a critical role in preserving the systemic stability of the financial system. It would present <u>systemic risk</u> and/or affect public or investor confidence should they be unable to complete (recover) and carry-on (resume) critical functions and activities.
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.

SECTION 3 : PRINCIPLES

Principle 1: Board and management should take responsibility for the BCP preparedness of their institution.

3.1 The planning for business continuity of an institution is the responsibility of the Board and management. Management should demonstrate, through regular attestation of their institution's BCP preparedness, that they have sufficient awareness of the risks and mitigating measures.

3.2 The attestation should state clearly the:

- Preparedness of the institution and
- Extent of alignment with the principles in this Paper taking into account the institution's level of business activities, risk management policies and role in preserving the systemic stability of the financial system.

3.3 The attestation should be addressed to the Board. Changes in the institution's business priorities might affect the effectiveness of their BCP preparedness. The attestation should therefore be updated regularly.

3.4 Increasingly, customers and counterparties are also seeking assurances on the BCP preparedness of the institutions that they have financial dealings with. Where appropriate, the attestation should be shared with customers, counterparties and other relevant parties.

Questions

- Q1 Would management attestation provide sufficient comfort and assurances to customers, counterparties or stakeholders of the institution's preparedness?*
- Q2 Should the attestation also indicate the residual risk(s)⁷, if any, that stakeholders, such as, the Board are prepared to tolerate?*
- Q3 Stakeholders and customers may need regular assurances on the institution's preparedness. Is an annual sign-off an appropriate frequency? If not, what would be an acceptable frequency to stakeholders and customers?*

Principle 2: Institutions should embed BCP into their business-as-usual operations, incorporating sound practices.

3.5 BCP is a risk-focussed and proactive process that includes understanding the entire ramification to the business, incident response, crisis management and external communications. It addresses operational risks by developing processes and procedures for the recovery of critical business functions to fulfil business obligations.

⁷ Risks that remain after mitigating measures have been applied.

3.6 A BCP should be credible, have a clear strategy and accountability, be practical in operation, updated as the business changes and meaningfully tested. Depending on the scale and scope of the institution's business, sound practices include:

- Clear BCP policy and strategies
- Clear roles and responsibilities to oversee the BCP programme
- Business impact analysis process
- Programme for the development, implementation, testing and maintenance of BCP
- On-going employee awareness and training programmes
- Procedures for emergency response and operations
- Procedures for external communications and crisis management coordination
- Procedures for coordination with external parties (including authorities, interdependency parties, etc.)

3.7 Once a BCP is established, it should be regularly reviewed, maintained and tested to ensure its currency, effectiveness and operational viability. Institutions should strive to build an organisational culture of embedding risk-focussed BCP into their business-as-usual operations and day-to-day management.

Q4 This principle calls for integrating risk-focussed BCP mindset into the fabric of an organisation. However, it is common practice that BCPs are developed on a cost-benefit basis.

Can institutions afford not to develop more risk-focussed BCP, taking into account the interests of their Board and stakeholders?

Q5 Are there any other essential BCP processes that should be included?

Principle 3: Institutions should test their BCP regularly, completely and meaningfully.

3.8 The effectiveness of the BCP needs to be assured through testing. Changes to technology, business processes and staff's roles and responsibilities would affect and impact the effectiveness of the BCP and ultimately the preparedness of the institution. Therefore, it is important that BCP be tested to measure its practicality and effectiveness. Tests will also serve to familiarise staff with the location of the recovery site, as well as the recovery procedures required during a disruption. The aim is to seek assurance that should institutions activate their BCP, they would be able to continue to operate reliably, responsively, and as efficiently as planned.

3.9 **Regular:** Institutions should test their BCP at least once a year. Frequent testing is a vital element of effective BCP. Some institutions have found that monthly or quarterly testing has helped considerably in their preparation for

dealing with disruptions. Management should participate in these tests and be familiar with their roles and responsibilities in the event of activation.

3.10 Complete and meaningful: All components of a business process should be meaningfully tested (e.g. from front-line through to supporting and processing components) which should include testing the connectivity, functionality and load capacity of the infrastructure provided at the recovery site(s). Institutions should satisfy themselves that their test programmes adequately cover both the qualitative and quantitative aspects. All strategic and planning assumptions should be regularly challenged to ascertain their applicability, especially with regard to changes in business scope or direction. Completeness would also include measuring the awareness and preparedness of personnel and coordination with external parties. Interdependencies, especially with external parties beyond institutions' control, should be thoroughly tested. This would include the institutions' offices, branches or service providers based outside of Singapore.

3.11 Other tests may include:

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

Formal test documentation and post mortem reviews listing lessons learnt and risk mitigating measure should be prepared for management sign-off.

3.12 Industry-wide: Appropriately scaled and coordinated tests between financial utility providers⁸ and their member institutions. This increases the level of awareness and confidence in recovery operations. Member institutions should participate in these tests.

Q6 Effectiveness of the BCP needs to be assured through testing. Are annual BCP tests, an appropriate frequency?

Q7 What role should industry associations or financial utility providers play in industry-wide BCP tests?

Q8 Are there other measurable determinants of complete and meaningful test?

⁸ Financial utility providers are organisations that provide specialised financial services such as clearing and settlement functions etc.

Principle 4: Institutions should develop recovery strategies and set recovery time objectives for critical business functions.

3.13 The establishment of recovery strategies would enable institutions to execute their BCP in an orderly and predefined manner that minimises disruption and financial loss. It forms the basis for defining recovery time objectives⁹ for their 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

3.14 In a crisis, it might not be practical to recover all business functions. Institutions should therefore identify their critical business functions and the potential losses (in monetary and non-monetary terms) should their operations be disrupted. A common process used to obtain this information is through a business impact analysis (BIA)¹⁰. 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.

3.15 Critical business functions differ among institutions due largely to their different business focus, markets, and customers' expectations. However, functions related to completing large-value payment instructions, clearing and settling material transactions, fulfilling material end-of-day funding and collateral obligations, managing customers' risk positions, and maintaining customer, investor or public confidence would generally be considered critical.

Recovery time objectives

3.16 While recovery time objectives may range from intra-day to within minutes of the disruption between institutions, significantly important institutions are expected to have faster recovery capabilities as compared with other institutions.

3.17 Recent discussions with some institutions indicated that the critical business functions of significantly important financial institutions should take less than four hours to recover from the time of disruption.

3.18 In addition, financial utility providers should recover and resume their critical business functions faster than the member institutions they provide services to, in order that members (affected or unaffected) may continue to operate. Failing which, they are likely to contribute towards the amplification of systemic risk.

⁹ The maximum acceptable length of time that can elapse before the lack of a business function severely affects the business entity. It comprises two components: the time before a disaster is declared, and the time to perform tasks to the point of business resumption.

¹⁰ Besides determining the potential losses, the BIA can also be used to identify the recovery priorities, resources required for recovery, critical staff and possible recovery strategies (how many recovery seats, 'Hot' or 'Cold' seats, etc.).

3.19 Recent discussions with some institutions indicated that the critical business functions of significantly important financial utility providers should take less than two hours, from the point of disruption, to recover and resume operations.

Q9 What factors should institutions consider when determining critical business functions?

Q10 It is important that significantly important institutions recover their critical business functions quickly.

Is a four-hours and two-hours recovery time objective reasonable for significantly important financial institutions and financial utility providers respectively?

Principle 5: Institutions should understand and appropriately mitigate interdependency risks of critical business functions.

3.20 There is a growing tendency for institutions to slice up and redistribute risk and processes locally, regionally or globally. This has led to increased dependency on other parties (internal or external). Any mismanagement of interdependency risk could cascade into operational or systemic inefficiencies, potentially leading to the failure of institutions.

3.21 When planning for the business continuity of critical business functions, institutions should take into account the interdependencies of these 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, especially their BCP preparedness and recovery priorities.

Examples of such dependencies are;

- ❑ Within an institution (e.g. Treasury, custody services)
- ❑ Between institutions (e.g. for US Dollar clearing)
- ❑ On financial utility providers (e.g. SGX, SWIFT)
- ❑ On vendors (e.g. disaster recovery service providers)
- ❑ On infrastructure providers (e.g. telecommunication)

BCP should take these complex dependencies into consideration and mitigate the risks as far as practically possible. Such dependencies should be factored in when institutions develop their recovery strategies and recovery time objectives.

3.22 Although some of the interdependency risks are beyond the institutions' direct control to mitigate completely (e.g. unavailability of telecommunication networks), this does not dilute the expectations of the institutions' services and obligations on the part of their customers and counterparties. Ultimately, the risk of interdependency lies with the institutions and cannot be "assumed" away. Therefore, institutions should take reasonable steps to mitigate such risks (e.g. initiate discussions with telecommunications provider to ensure communication lines are routed through different exchanges).

3.23 Before contracting with any external service providers, institutions should satisfy themselves that the risk of outsourcing remains within acceptable operational risk policies and that it does not compromise their own BCP. They should ensure that their service providers have contingency plans in place that are equal to, if not more robust than, their own BCP preparedness. Institutions should also proactively seek assurances from their service providers that their BCP are regularly tested.

3.24 In the event of an unexpected termination or liquidation of the external service provider, the interim risk to institutions may be unacceptable as finding another suitable provider may take many months to secure and implement. 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 and maintain the sanctity of their BCP.

Q11 Should interdependency risks with external service providers be addressed on an individual institution basis or industry basis?

Q12 How feasible is it for institutions to mitigate risk against unexpected termination or liquidation of their external service providers?

Principle 6: Institutions should plan for wide-area (zonal) disruptions.

3.25 The September 11 event has demonstrated that institutions should plan for disruptions that impact a wide area (zone). A zone is defined as a reasonable area¹¹ that could be affected by the same disruption. Institutions should also cater for scenarios where there are significant loss or inaccessibility of critical staff, or where there is a widespread disruption of critical services such as telecommunications. Institutions should decide on the need to cater for multiple zone outage scenarios in their BCP, taking into account their respective levels of critical business activities, risk tolerance and risk management policies. In addition, they should consider broadening and deepening their BCP scope to cater for scenarios of longer disruptions.

3.26 Zonal disruptions may heighten interdependency risks. Interdependencies between critical functions and services providers within the same zone have to be mitigated appropriately. For institutions with customers, counterparties and service providers whose primary sites are also within the same zone, telecommunication links should also be arranged between their recovery site(s). These links should be tested.

Q13 In the context of Singapore, what would be a reasonable distance to define zone for BCP purposes?

Q14 Besides distance, are there any other indicators that could be used to separate the primary and recovery locations of critical functions and people?

¹¹ The definition of a zone should at least cater for a scenario where the entire Central Business District (which is about two-kilometres diameter) is affected by the same disruption.

Principle 7: Institutions should practise separation policy to mitigate concentration risk.

3.27 Critical staff and information are important assets that are difficult to replace quickly. Institutions should assess their concentration risk when business operations and technology (IT equipment and staff) are housed within the same zone. Many institutions today, for example, 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 the case as disruptions may also result in the unavailability of critical staff.

3.28 It is important therefore, to find the right balance between mitigating concentration risk and increasing human safety, and that of not losing the efficiencies gained from the centralisation of business processes and critical staff. In preparing for zonal disruptions, institutions should endeavour to adopt the following three separation policies for their critical business functions.

3.29 Firstly, **primary-recovery site separation**. The primary site of the critical business function and the recovery site should be in different zones. For example, Treasury dealing functions and their recovery site should be situated in different zones.

3.30 Secondly, **separation of transaction operations¹² and IT operations**. Critical transaction operations and their supporting IT operations should be in different zones. For example, settlement operations staff and their IT operations (includes IT equipment and staff) should be in different zones.

3.31 Thirdly, **intra-function separation**. Another labour pool that is able to take over the critical business functions should be available in a different zone. Solutions may include separating staff between the two operational sites and cross-training staff in another zone. Institutions should determine and design the most appropriate combination of mitigating measures that minimises the concentration risk. Institutions are encouraged to be innovative and to explore different means of implementing this principle.

Q15 Are the separation policies relevant in mitigating concentration risks? If not, why? Would customers and stakeholders agree with you?

Q16 Are the three separation policies equally important? If not, why? Would customers and stakeholders agree with you?

Q17 Are there other compensating alternatives that may mitigate this risk?

¹² Sometimes referred to as backroom or back-office operations.

APPENDIX A – SPECIFIC LESSONS FROM SEPTEMBER 11

A.1. While the global financial markets quickly returned to normal operations in the aftermath of September 11, the incident highlighted several key vulnerabilities within the U.S. financial sector that also exist in financial centres around the globe. Singapore, as an international financial centre, is plugged into this global network and institutions here cannot afford to ignore the lessons learnt. Some of these were:

A.2. **Extend scopes of scenarios:** Traditionally institutions do not plan for scenarios beyond single building outages. September 11 has changed this paradigm as institutions are now planning for wider area impact and greater physical disruptions. Planning for loss or inaccessibility of critical staff or widespread telecommunication disruptions was also generally not considered in the past. Going forward, CBD-wide or prolonged disruptions could be the benchmark for planning purposes.

A.3. **Concentration risk:** The significant presence of institutions within a geographic area invariably leads to single-point-of-concentration which may intensify the impact of any disruption. This impact may even be compounded if some critical market functions such as clearing and settlement were dependent on one or two institutions whose operations are also situated in the same geographic area, or where contingency plans rely on the same labour pool to perform recovery services. These factors combined could have broad and systemic implications for the financial sector. As such, separation policies with respect to business process, technology and people may have to be considered.

A.4. **Interdependency risk:** Interdependency risks that exist between institutions, or between external service providers (e.g. Telecommunication firms and disaster recovery vendors) and institutions would need to be mitigated appropriately. It also highlighted the need for greater assurance through coordinated testing (including industry-wide testing). This unfortunately is not a common practice. Testing that is regular, complete and meaningfully executed would go a long way to improving the effectiveness of BCP.

A.5. **Tier business recovery:** Some operations (e.g. clearing and settlement) and financial utility providers (e.g. payment systems and infrastructure providers) can be considered so vital that they must recover and continue with minimal disruption, if any, even in the event of a wide-area disaster. Establishing recovery and resumption time objectives may be necessary for critical business operations and significantly important institutions.