November 2007

Recommendations for
Business Continuity Management (BCM)
Recommendations for Business Continuity Management (BCM)

Contents

1. Background and objectives............................................................................................................... 2
2. Link with the BCP Swiss Financial Centre working group.......................................................... 2
   2.1 Fundamentals.................................................................................................................................. 2
   2.2 Framework conditions ..................................................................................................................... 3
3. Principles....................................................................................................................................... 3
4. Scope of application and scenarios............................................................................................... 4
5. Recommendations............................................................................................................................. 4
   5.1 Definition and scope......................................................................................................................... 4
   5.2 Components ................................................................................................................................... 5
   5.3 Responsibilities ............................................................................................................................... 6
   5.4 Business Recovery Planning and review thereof ............................................................... 6
      5.4.1 Business Impact Analysis (binding minimum standard)......................................................... 6
      5.4.2 Business Continuity Strategy (binding minimum standard)............................................... 7
      5.4.3 Business Continuity Plans....................................................................................................... 7
      5.4.4 Business Continuity Reviews................................................................................................. 7
      5.4.5 Business Continuity Tests....................................................................................................... 7
   5.5 Crisis management ....................................................................................................................... 7
   5.6 Reporting, communication and training ...................................................................................... 8
      5.6.1 Reporting .................................................................................................................................. 8
      5.6.2 Communication ......................................................................................................................... 8
      5.6.3 Training and awareness ............................................................................................................. 8
6. Entry into effect and transitional arrangements............................................................................. 8

Appendix A - Glossary.......................................................................................................................... 9
Appendix B - Severity of events......................................................................................................... 11
Appendix C - Development of a crisis ............................................................................................... 12
Appendix D - Sources of further information................................................................................... 13
1. Background and objectives

Various events of recent years, particularly in connection with terrorism and pandemics, have highlighted the vulnerability of financial market participants and financial systems. Awareness of such events and their potential impact has increased significantly.

As a result, international organisations and the governments of various countries have drawn up guidelines and recommendations in the area of Business Continuity Management (BCM) together with requirements for financial market participants and supervisory authorities.

The Swiss Federal Banking Commission (SFBC) views appropriate Business Continuity Management as a prerequisite for the granting of an operating licence in accordance with Art. 3 of the Banking Act. It supports the corresponding self-regulatory guidelines issued by the Swiss Bankers Association (SBA).

The SBA's self-regulatory guidelines are aimed at its members and contain "best-practice" recommendations to be used in the preparation of an institution-specific BCM policy. Any policy should take account of the specific circumstances of the institution in question, in particular its risk situation and systemic relevance.

This document essentially takes the form of recommendations, compliance with which is not binding in the sense of SFBC Circular 04/2, “Self-Regulation as a Minimum Standard”. The completion of a Business Impact Analysis (section 5.4.1) and the definition of a Business Continuity Strategy (section 5.4.2) are exceptions to the above. The SFBC views these two core elements as binding minimum standards under supervisory law.

These recommendations apply to banks and securities dealers (hereinafter referred to as institutions). They are not intended to have any impact on the relationship between institutions and their clients under civil law.

2. Link with the BCP Swiss Financial Centre working group

2.1 Fundamentals

In order to deal with unforeseen incidents in the networked financial system, it is vital that all major players adopt a coordinated approach and define, harmonise and implement the necessary measures before such incidents arise.

The BCP Swiss Financial Centre working group, composed of representatives of the financial market's stakeholders and chaired by the Swiss National Bank (SNB), has been active in Switzerland since December 2003. The aim of the working group is to review and assess the current Business Continuity Plans of individual institutions and infrastructure providers of the Swiss financial centre. Its investigation has focused on the processes critical to ensuring the stability of the financial centre.

Based on an initial risk analysis, the working group has identified “settlement of large value payments via Swiss Interbank Clearing SIC” and “liquidity provision via repo” as the two processes that are critical to ensuring the stability of the financial centre. Other areas such as retail payments, cash supply for the public and stock exchange trading were not rated as priorities in this regard. Following the investigation the central infrastructures Telekurs/SIC and SIS were commissioned by the SNB to incorporate BCM requirements into their contractual agreements with participants.
2.2 Framework conditions

Taking its cue from the corresponding guidelines of the Federal Reserve System (Fed, see Appendix D), the working group has laid down the following requirements for the two core processes “settlement of large value payments via Swiss Interbank Clearing SIC” and “liquidity provision via repo” (definitions provided in Appendix A):

<table>
<thead>
<tr>
<th>Participants in financial system</th>
<th>Recovery objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central infrastructures (SNB, SIC and SIS)</td>
<td>RTO &lt;= 2h</td>
</tr>
<tr>
<td>Critical system participants</td>
<td>RTO &lt;= 4h</td>
</tr>
<tr>
<td>Other system participants</td>
<td>RTO &lt;= 24h</td>
</tr>
</tbody>
</table>

System participants with a market share of 20% or more in SIC are considered to be “critical”. In line with this terminology, all other system participants are deemed to be “other system participants”. The time guidelines for (critical and other) system participants apply explicitly to the core “large value payments” and “liquidity provision” processes; they may also be achieved via alternative processes. It should be borne in mind that crises and the steps to deal with them can last several days or weeks, and corresponding capacity must therefore be available. The guideline of 24 hours for other system participants is a standard that can be adjusted by individual institutions in accordance with their specific BCM strategy (documented risk assessment). The SFBC Circulars “Supervision and Internal Control” (06/6) and “Capital Adequacy for Operational Risks” (06/3) are also authoritative in this context.

The specific recovery objectives are set out in the technical instructions to the agreements between the central infrastructure providers and system participants.

3. Principles

These recommendations are based on various sets of comparable standards (see the overview in Appendix D), in particular the “High-Level Principles for Business Continuity” of the Joint Forum/Basel Committee on Banking Supervision (Bank for International Settlements, August 2006, www.bis.org).

The key elements of these “High-Level Principles” can be summarised as follows:

1. Financial market participants and supervisory authorities should have an effective and comprehensive Business Continuity Management process at their disposal. Responsibility for ensuring business continuity lies with the Board of Directors and Senior Management.
2. Financial market participants and supervisory authorities must integrate the risk of significant operational disruptions into their Business Continuity Management processes.
3. Financial market participants must develop recovery objectives that take account of their systemic relevance and the resulting risk for the financial system.
4. The Business Continuity Plans of both financial market participants and supervisory authorities must define internal and external communication measures in the event of major business interruptions.
5. Where business interruptions have international implications, the corresponding communication concepts must cover in particular communication with foreign supervisory authorities.
6. Financial market participants and supervisory authorities must test their Business Continuity Plans, evaluate their effectiveness and amend their Business Continuity Management processes where necessary.
7. It is recommended that supervisory authorities assess the Business Continuity Management programmes of the institutions subject to supervision as part of the ongoing monitoring process.

4. Scope of application and scenarios

Institutions must take into account all potentially relevant scenarios that could result in a crisis for the company. The term “crisis” denotes a threatening situation that calls for critical decisions and cannot be handled with ordinary management tools and decision-making powers. Consequently, the management of “incidents” is expressly not covered by these recommendations (“Availability Management”, see definitions in Appendix A and Appendix B). The following are examples of crisis situations:

- “Accident-like” events such as fires or explosions
- Terrorist attacks, sabotage
- Natural disasters such as floods or earthquakes
- Mass absence of personnel, e.g. due to a pandemic
- Failure of building technology and/or energy supply (e.g. electricity)
- Failure of IT systems or infrastructures (hardware or software errors)
- Failure of communication systems or telecom providers
- Failure of external suppliers (cf. outsourcing) such as information providers.

As part of BCM, the relevant threats/crisis types are to be identified/defined and assessed by the institutions in terms of their relative impact (severity) and probability of occurrence.

One key consequence of such events may be that staff and/or infrastructure (primarily management infrastructure, telecommunication, buildings or workstations) are no longer available for business-critical functions. In addition, problems with IT services or infrastructure providers can result in intolerable periods of downtime for critical services.

In the area of pandemics, damage scenarios and recommendations are set out in a number of documents including the “Swiss Influenza Pandemic Plan 2006” (Chapter 8, “Companies”) issued by the Federal Office of Public Health (FOPH) (www.bag.admin.ch/influenza).

BCM must ensure optimum compliance with legal, regulatory, contractual and internal provisions even in crisis situations.

5. Recommendations

5.1 Definition and scope

Business Continuity Management (BCM) is a company-wide approach designed to ensure that critical business functions can be maintained or restored as quickly as possible in the event of internal or external incidents. One of the aims of BCM is therefore to minimise the financial, legal and reputational impact of such incidents.

Overall, BCM is intended to ensure the continuation or rapid recovery of business activity in crisis situations. As a result, BCM essentially involves all business and organisational areas within a company. A distinction must be made between advance business recovery planning and crisis management in real cases.
In its Business Continuity Strategy an institution defines its fundamental procedures in the event of a failure of critical resources. A Business Impact Analysis is carried out to identify business-critical resources and processes; this will include defining appropriate recovery times and availabilities. The Business Continuity Strategy forms the basis for the Business Continuity Plans. These define (in the sense of preparatory measures, checklists and work tools) the procedure for the timely and correct recovery of business activity. The Business Continuity Strategy can be an integral component of an institution’s corporate strategy. The strategy must provide explicit information on any specific residual risks that are consciously accepted.

The development and implementation of a BCM process will focus in particular on the following areas:

- Definition including scope of BCM
- Anchoring of BCM in the corporate organisation
- Creation of a governance structure adapted to the corporate organisation
- Definition of BCM roles and responsibilities
- Definition of crisis scenarios (see Chapter 4) and their impact on the company’s resources (planning basis)
- Identification of business-critical resources and processes together with an analysis of the impact of losing them by means of a Business Impact Analysis (BIA)
- Definition of the Business Continuity Strategy for the fundamental approach to dealing with losses of individual business architecture resources
- Preparation of Business Continuity Plans designed to permit the recovery of business-critical processes and resources in a crisis situation
- Business Continuity Reviews and Business Continuity Tests for the Business Continuity Plans and crisis management organisation
- Reporting, communication and training.

5.2 Components

A crisis situation is characterised by the complete or partial failure of resources or an interruption to one or more processes. In principle, the availability of the following resources is a prerequisite for the execution of processes:

- Staff
- Buildings
- IT/data
- External suppliers.

With this in mind, it is recommended that Business Recovery Planning focus primarily on the failure of these resources.

BCM should first and foremost include the following components:

<table>
<thead>
<tr>
<th>Business Impact Analysis</th>
<th>Identification of business-critical processes and the underlying critical resources, identification and description of the impact of the failure of one or more critical resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity</td>
<td>Definition of the fundamental procedure in the event of a failure of critical resources, fundamental decisions on the provision of replacement resources.</td>
</tr>
<tr>
<td>Strategy</td>
<td></td>
</tr>
</tbody>
</table>
Business Continuity Plans

Comprehensive set of measures to ensure the continuation of business activity or the rapid recovery of critical processes. Detailed plans of procedures and responsibilities in the event of a failure of critical resources.

Business Continuity Testing

Regular reviews of Business Continuity Plans to ensure they are up-to-date, implementable and effective.

Crisis management organisation

The aim of crisis management organisation is to provide a crisis management framework to enable the company to deal effectively with crisis situations.

BCM reporting

Reporting on BCM activities and the current status of the company’s crisis management preparations (including to the Board of Directors and Senior Management).

BCM training

Technical BCM training for staff who have taken on BCM responsibilities.

BCM communication

Measures to safeguard internal and external communication in the event of a crisis.

5.3 Responsibilities

Responsibility for BCM lies with the Board of Directors and Senior Management of each individual institution (see also the SFBC Circular “Supervision and Internal Control”, 06/6).

The Board of Directors is responsible for monitoring compliance with a documented BCM strategy. The Senior Management sets out this strategy and regulates other responsibilities, authorities and information flows in internal rules and directives. In particular, the Senior Management (with approval from the Board of Directors) governs the relationship between Senior Management and the crisis organisation (Crisis Management Team).

5.4 Business Recovery Planning and review thereof

5.4.1 Business Impact Analysis (binding minimum standard)

Each business area should determine its critical resources and processes. For business-critical processes, the impact of a complete or partial failure of the corresponding resources is assessed by means of an impact analysis.

This assessment also considers mutual interdependencies between business areas (up/downstream processes) and dependencies in connection with external providers (outsourcing).

The analysis is intended to indicate:

- the desired extent to which business-critical processes are to be recovered
- the maximum period until the recovery of business-critical processes
- the minimum scope of (replacement) resources (buildings, staff, IT/data, external providers) that must be available in the event of a crisis in order to achieve the desired level of recovery.

The frequency with which the Business Impact Analysis is updated is determined primarily by the risk situation of the institution in question.
5.4.2 Business Continuity Strategy (binding minimum standard)

The Business Continuity Strategy lays down the fundamental procedure with which the company intends to achieve the recovery objectives for the underlying scenarios and their impact on resources identified in the Business Impact Analysis. This strategy is to be documented in writing.

5.4.3 Business Continuity Plans

Business Continuity Plans describe the necessary procedures for the recovery or continuation of business-critical processes (including compliance with legal, regulatory, contractual and internal provisions), replacement solutions and the minimum replacement resources they require. Corresponding plans should at least contain: A description of the case of application (trigger scenario), procedure/prioritised catalogue of measures, necessary replacement resources and crisis organisation indicating responsibilities and authorities.

Regular time periods should be specified within which the Business Continuity Plans are to be updated. Significant changes to business operations may also necessitate an overhaul of the plans.

5.4.4 Business Continuity Reviews

Business Continuity Reviews include a status report on the BCM documentation prepared by the various business areas together with an evaluation of whether the documents meet the defined review criteria. It is advisable to define consistent review criteria and a clear process for monitoring and remedying outstanding issues.

5.4.5 Business Continuity Tests

Business Continuity Tests are used to test and review implementation of Business Continuity Plans and the capability of the crisis management organisation. The focus and frequency of individual tests is determined by the risk assessment (cf. Business Impact Analysis). By aggregating the test results from individual organisational units, the institution’s capacity to deal with crisis situations can be assessed.

It is advisable to coordinate individual test activities in the form of a systematic testing plan, ensure standardised reporting and lay down a process for monitoring and remedying of weak spots.

5.5 Crisis management

The aim is to provide a crisis management framework that enables the company to deal with crisis situations effectively and as quickly as possible. In crisis situations that call for critical decisions and cannot be handled with ordinary measures and decision-making powers, the Crisis Management Team(s) is/are convened. They take over responsibility for managing the crisis until order is restored.

It is advisable to clearly set out the responsibilities and authorities of the Crisis Management Team as well as the circumstances under which it is to be convened in advance and gear crisis organisation to the institution’s business activity and geographical structure. Particular emphasis should be placed on ensuring optimum contactability for people in positions of responsibility even in crisis situations.
5.6 Reporting, communication and training

5.6.1 Reporting

Appropriate reports on BCM activities and the status of crisis management preparations in general are to be prepared for the Board of Directors and Senior Management at pre-defined intervals. These should include in particular the results of Business Continuity Reviews and Business Continuity Tests.

5.6.2 Communication

Communication plays a key role in crisis management. Special attention must therefore be paid to the systematic and careful preparation of communication concepts and plans (internal and external communication) in the event of a crisis. Particular attention should be paid to ensuring a high degree of professionalism and maintaining credibility and trustworthiness versus dialogue partners.

Communication plans must contain information on availability in the event of a crisis (list with names and telephone numbers of supervisory authorities, staff, media, clients, counterparts, service providers, etc.). Special communication measures must be incorporated if there is an international dimension.

The supervisory authority is to be notified accordingly in the event of a crisis or if the crisis organisation is triggered.

5.6.3 Training and awareness

Care must be taken to ensure that staff receive sufficient training regarding their duties, responsibilities and authorities in connection with their respective BCM activities. This covers both training for new staff and regular training updates for existing staff. Special attention must be paid to the training given to members of the crisis organisation.

In addition, both new and existing staff are to be made aware of the importance of BCM with the aid of an ongoing information programme.

6. Entry into effect and transitional arrangements

These recommendations were adopted by the SBA’s Board of Directors in its resolution of 18 June 2007 and approved by the SFBC on 19 October 2007. They enter into effect on 1 January 2008. The institutions are advised to implement the content of the recommendations at the latest by 31 December 2009.
Appendix A - Glossary

Availability Management: Procedure involving the definition, analysis, planning, measurement and optimisation of all factors influencing the availability of IT services. Availability management ensures that the entire IT infrastructure and all IT processes, tools, tasks, etc. meet the availability requirements defined in the Service Level Agreements. Incidents that affect availability can be controlled with normal management processes and decision-making powers.

Backlog Processing: Retrospective handling of uncompleted or backlogged work due to an interruption in business processes or the implementation of alternative processes.

Business Continuity Management (BCM): Company-wide management approach (policies and standards) designed to ensure that critical business functions can be maintained or restored as quickly as possible in the event of (internal or external) incidents. BCM therefore encompasses the planning, implementation and controlling phases and covers the entire associated environment (areas, processes, technologies) required to ensure that following an incident (business-)critical processes are continued without interruption or recovered within a defined time period.

Business Continuity Plans: Comprehensive, prepared set of measures (including checklists and work aids) designed to facilitate continuous business activity or the orderly and rapid recovery of (business-)critical processes in the event of a crisis.

Business Continuity Reporting: Reporting (including to the Board of Directors and Senior Management) on Business Continuity Management activities, particularly the status of crisis management preparations. In particular, Business Continuity Reporting must present the results of Business Continuity Reviews and Business Continuity Tests.

Business Continuity Strategy: Definition of the fundamental procedure for maintaining or restoring continuous business activity in the event of a failure of critical resources (including a definition of risk acceptance, analysis of potential courses of action and fundamental decisions on the provision of replacement resources). The Business Continuity Strategy is based on the Business Impact Analysis and forms the basis for Business Continuity Plans.

Business Continuity Testing: Regular, systematic review of Business Continuity Plans, particularly with regard to their implementation and effectiveness and how up-to-date they are.

(Business-)critical processes: The processes within a company the failure of which makes it impossible or extremely difficult to maintain client services, comply with the company’s legal obligations and/or manage its risk positions and can hence result in critical (direct or indirect) losses.

Business Impact Analysis (BIA): Identification and (quantitative and qualitative) measurement of the impact of interruptions in business activity or the failure of individual resources and/or processes. In particular, the BIA serves to identify (business-)critical resources and processes based on an analysis of dependencies and impacts as well as an evaluation and classification of potential damages.

Business Recovery: Recovery of specific processes or business activities following an interruption, or measures to be taken following a loss event (cf. Business Continuity Plans).

Business Resumption: Temporary solutions for business processes employed in order to resume business activity. They can be applied on a step-by-step basis until ordinary business activity or full capacity is recovered.
Crisis: Threat situation that calls for critical decisions and cannot be handled with ordinary management tools and decision-making powers.

Crisis Management Team: Team responsible for crisis management in the event of a crisis up to the point when order is restored (minimising economic damage and reputational risks).

Critical resources: Those resources of a company (staff, buildings, IT/data, external suppliers) whose failure results in the interruption or failure of (critical) business processes. Critical resources are identified in the Business Impact Analysis.

Incident: Event that results in an interruption to business activity, loss and/or impairment of service quality, but (in contrast to a crisis) can be handled through availability management.

Recovery Point Objective (RPO): Defined, maximum acceptable data loss in the event of a crisis.

Recovery Time Objective (RTO): Defined period within which (business-)critical processes must be recovered.
Appendix B - Severity of events

Depending on the severity of the consequences arising from one or more events, it/they is/are referred to as an incident, a major incident, a crisis or a disaster. Business Continuity Management is only concerned with crisis and disaster planning and crisis management.

Disaster: A major incident, having critical impact on the company and affecting the corporate value system, will be declared a disaster by the responsible crisis management team. A disaster is primarily handled by activation of the business recovery plans.

Crisis: A threat that requires critical decisions which cannot be resolved with ordinary management techniques and decision-making authority.

Major Incident: The consequence of one or more incidents, for which the cause might be unknown, but have significant impact on business operations.

Incident: An event that leads to (or may lead to) a business disruption, a failure, a loss or a limitation of service quality. The type and severity of the incident cannot be usually specified exactly when taking notice of the damage.
Appendix C - Development of a crisis

Development of a crisis using the example of the impact type “Loss of IT/data”
Appendix D - Sources of further information

The following standards can be consulted when implementing Business Continuity Strategies and Plans. The list is not exhaustive.


