SwissBanking

August 2013

Recommendations for Business Continuity Management (BCM)

Contents

1 Background and objectives

Various events in recent years, particularly in connection with terrorism, pandemics and natural disasters, 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 governmental bodies of various countries have drawn up guidelines and recommendations in the area of Business Continuity Management (BCM) containing requirements for financial market participants and supervisory authorities.

The Swiss Financial Market Supervisory Authority FINMA considers appropriate Business Continuity Management as a prerequisite for granting an operating licence according to Art. 3 of the Banking Act and 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. Policies should take account of the specific circumstances of the institution in question, in particular its risk situation and systemic relevance.

Three sections of these Recommendations are recognised by FINMA in its Circular 2008/10 "Self-regulation as a minimum standard" and are regarded as binding minimum standards under supervisory law, compliance with which is verified by auditors. The definition of a Business Continuity Management Strategy (section 4.4), the completion of a Business Impact Analysis (section 4.5.1) and the formulation of Business Recovery Options (section 4.5.2) are binding.

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

2 Principles

These Recommendations are based on various sets of comparable standards (see sources of further information in Appendix D). They are based in particular upon

- the "High-Level Principles for Business Continuity" of the Joint Forum and Basel Committee on Banking Supervision[1]
- the "British Standard for Business Continuity Management BS 25999"[2] and ISO 22301[3].

The aforementioned "High-Level Principles" set out the following recommendations:

1. Financial market participants and supervisory authorities should have an effective and comprehensive Business Continuity Management program at their disposal. Ultimate responsibility for Business Continuity Management lies with an organisation's Board of Directors and Senior Management.
2. Financial market participants and supervisory authorities are advised to integrate the risk of significant operational disruptions into their Business Continuity Management program.
3. Financial market participants are advised to define recovery time objectives (RTOs) that take account of their systemic relevance and the resulting risk for the financial system.
4. Financial market participants and supervisory authorities are advised that their Business Continuity Plans should define internal and external communication measures for use in major business interruptions.
5. Where business interruptions may have international implications, it is advised that the corresponding communication measures address in particular communication with foreign supervisory authorities.

[1] Basel Committee on Banking Supervision, Bank for International Settlements, August 2006, www.bis.org.
[2] British Standards Institution, September 2008, www.bsigroup.com.
[3] International Organization for Standardization (ISO), May 2012, www.iso.org.

6. Financial market participants and supervisory authorities are advised to test their Business Continuity Plans, evaluate their effectiveness and amend their Business Continuity Management processes accordingly where necessary.
7. Supervisory authorities are called upon to incorporate Business Continuity Management reviews into their frameworks for the ongoing surveillance of the financial institutions for which they are responsible.

Furthermore, the results produced by the working group "Business Continuity Planning in the Swiss Financial Centre", which was chaired by the Swiss National Bank should be taken into account, in particular the two processes "settlement of large value payments via SIC" and "liquidity provision via repo", which have been identified as critical.[4]

3 Scope of application and threats

Institutions must take into account all potentially relevant threats that could result in a crisis for the company. The term "crisis" denotes a threat situation that require critical decisions and cannot be handled with ordinary management tools and decision-making powers. In this sense, the management of "incidents" is expressly not part of these Recommendations (for "Availability Management", see definitions of terms in Appendices A and B). The following are examples of crisis situations:

- "Accident-like" events such as fires or explosions
- Terror attacks, sabotage
- Natural disasters such as floods or earthquakes

It is recommended best practice, however, that when a Business Continuity Management program is implemented, preparations focus primarily on the consequences and not the causes of crises. In respect of the recovery of critical business processes or business activities follow-

[4] Swiss National Bank (SNB), Business continuity in the Swiss financial sector, 2006 and 2009, www.snb.ch.

ing an interruption, the Business Recovery Options should take various impacts into consideration in accordance with the defined recovery objectives (see section 4.5.2).

As part of BCM, institutions must identify/define and assess the relevant threats in terms of their relative impact (severity).

A key consequence of such events may be that staff and/or infrastructure (buildings or workstations, management infrastructure, telecommunications) are no longer available for business-critical processes or are only available on a limited basis. In addition, problems with IT services or infrastructure providers can result in situations where business-critical processes can no longer be carried out.

In the area of pandemics, damage scenarios and recommendations from the Federal Office of Public Health (FOPH) need to be taken into account. Pandemic planning must take account of the fact that the impact of a major infectious disease can differ significantly from "classic" BCM crisis situations in duration and the extent to which outbreaks can be forecast.

BCM crisis situation

- arises unexpectedly and rapidly has a major impact on business operations, and
- planning focuses on the rapid recovery of the operating capacity

whereas in a pandemic

- there is a lengthier period of time until infections peak and
- planning is required for how critical business processes can be maintained and less critical business processes suspended.

It is recommended to produce a pandemic plan at least on an institutional level. Further information can be found on the corresponding FOPH homepage[5].

[5] Swiss Federal Office of Public Health, Swiss Influenza Pandemic Plan, January 2009, www.bag.admin.ch.

In many business processes, services are provided by external suppliers and service providers that could likewise fail or be disrupted suddenly. If external providers or suppliers support business-critical processes, their BCM maturity should be assessed within an appropriate framework.

Within the context of Business Recovery Options (section 4.5.2), one option is the transference of services from from external to internal service providers. Similarly, redundant or alternative providers can be called in on a precautionary basis.

In addition to FINMA Circular 2008/7, which deals with outsourcing at banks, it is recommended best practice that workaround solutions always be planned for the event that critical external service providers or suppliers fail.

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

4 Recommendations

4.1 Definition and scope

Business Continuity Management (BCM) is a company-wide approach designed to ensure that critical business processes can be maintained in the event of major 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, on a previously defined level of continuation or recovery. As a result, BCM essentially involves all business and organisational areas within a company. A distinction must be made between BCM planning measures which are defined in advance and actual crisis management in real situations.

4.2 Responsibilities

Responsibility for Business Continuity Management lies with the Board of Directors and Senior Management of each individual organisation (see also FINMA Circular 2008/24 "Supervision and internal control – banks").

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

4.3 Risk analysis

Within the framework of Business Continuity Management, either a risk analysis can be carried out for critical resources or reference can be made to existing risk analyses from other areas such as risk management. In BCM, a risk analysis is used to identify the potential threats that could cause an interruption of business processes. The underlying assumption in the BCM context is that such threats could arise. Even if it is not always possible to identify all possible risks in their entirety, this allows potential threats to be flagged up and assessed. Targeted measures could potentially be used to bring the likelihood of a crisis scenario down to an accepted level.

4.4 Business Continuity Management Strategy (binding minimum standard)

The institution uses the Business Continuity Management Strategy to define its fundamental approach to Business Continuity Management.

The Business Continuity Management Strategy can be an integral component of an institution's corporate strategy, or it can stand alone. The strategy must provide explicit information on any specific residual

risks that are consciously accepted. A written record must be kept of decisions taken in this regard.

The following aspects must be set out in the BCM Strategy:

- Definition of and determination of scope of BCM
- Anchoring of BCM in the corporate organisation
- Creation of a governance structure adapted to the corporate organisation
- Definition of roles and responsibilities in connection with BCM
- Definition of threats and their impact on the company's resources (basis for planning)
- Definition of the frequency with which reviews and tests of plans and measures will be carried out
- Definition of reporting, communication and training

4.5 Elements of Business Continuity Management

4.5.1 Business Impact Analysis (binding minimum standard)

The Business Impact Analysis (BIA) provides the requisite information on business-critical processes and resources. For these business-critical processes, the impact of a complete or partial loss of the corresponding resources is assessed as part of BCM. Each business area determines its critical resources and processes.

This assessment also considers interdependencies between business areas (process dependencies) and dependencies in connection with external service providers and suppliers (outsourcing).

This analysis, which is then used to formulate the recovery objectives, is intended to provide the following minimum results:

- the defined timeframe within which business-critical processes and/or IT services have to be recovered (Recovery Time Objective, RTO)
- the desired extent to which business-critical processes are to be recovered within the defined RTO

- the minimum scope of (replacement) resources (buildings, staff, IT/data, external service providers and staff) that must be available in the event of a crisis in order to achieve the desired level of recovery.

The BIA should be reviewed once a year, and the type and scope of this review should be geared in particular towards the institution's specific risk situation.

4.5.2 Business Recovery Options (binding minimum standard)

The Business Recovery Options set out at operational level the basic procedure by which the company – for the business areas selected in accordance with section 4.5.1 – aims to achieve the recovery objectives defined in its Business Impact Analysis for the underlying threats and their impact on resources. The recovery objectives should be recorded in writing and cover the recovery options defined for critical resources. As a minimum, the available Business Recovery Options in the event of a loss of

- staff
- buildings
- IT systems or IT infrastructure (including communications systems)
- external service providers and suppliers (outsourcing) such as information providers

should therefore be set out.

These Business Recovery Options should then be formulated in the various Business Recovery Plans. Acceptance of a residual risk can constitute a Business Recovery Option. This should be arrived at in the same way and recorded in writing.

4.5.3 Business Recovery Plans

Business Recovery Plans describe the procedures, replacement solutions and minimum replacement resources required for the continuity

and/or recovery of business-critical processes (including compliance with legal, regulatory, contractual and internal provisions). These plans should contain as a minimum: a description of the case of application (triggering threat), a procedure or catalogue of measures with priorities, and the replacement resources required.

Business Recovery Plans should be checked at least once a year to ensure they are up to date, and adapted where necessary. Plans may also need to be revised when there are significant changes to business operations (reorganisations, new business lines, etc.).

4.5.4 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 open issues.

4.5.5 Business Continuity Tests

Business Continuity Tests are used to test and review implementation of Business and IT Disaster Recovery Plans and the capability of the crisis management organisation. The focus and frequency of the individual tests should be determined on the basis of the criticality assessment (see Business Impact Analysis). By testing individual organisational units simultaneously, it is possible to assess an institution's overall capability to deal with crisis situations.

It is advisable to coordinate individual test activities under a systematic testing plan, ensure standardised reporting and lay down a process for monitoring and remedying weak points.

Planning should be structured in such a way that the most important measures (including the crisis organisation) can be practised and tested at least once a year.

4.6 Crisis management

The aim is to define a crisis management framework that enables the company to deal with crisis situations effectively and in a timely manner. In situations that require critical decisions and cannot be handled with ordinary measures and decision-making powers, the Crisis Management Team is convened. This team takes over responsibility for managing the crisis until a good working order is restored.

It is advisable to clearly set out the responsibilities and authorities of the Crisis Management Team and the circumstances under which it is to be triggered in advance and to gear the crisis organisation to the institution's business activities and geographical structure. Particular emphasis should be placed on ensuring optimum contactability for people in positions of responsibility, even in crisis situations.

4.7 Reporting, communication and training

4.7.1 Reporting

Appropriate reports on BCM activities and the status of crisis management preparations 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.

4.7.2 Communication

Communication plays a decisive role in crisis management. Special attention must therefore be paid to the systematic and careful preparation of communication concepts and plans (internal as well as external communication) for crisis situations. Particular attention should be paid to ensuring a high degree of professionalism and maintaining credibility and trustworthiness vis-à-vis the company's various stakeholders.

Communication plans should in particular ensure that certain people/parties can be contacted in a crisis (list with names and telephone

numbers of supervisory authorities, staff, media, clients, counterparties, service providers, etc.). If a crisis has an international dimension, special communication measures need to be taken into account.
The supervisory authority is to be notified accordingly in the event of a crisis or if the crisis organisation is triggered.

4.7.3 Training and awareness raising

An organisation needs to ensure that staff receive sufficient training regarding their duties, responsibilities and powers in connection with their BCM activities. This covers both training for new staff and regular refresher training 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 and kept aware of the importance of BCM by means of an ongoing information programme.

5 Entry into effect

These Recommendations were adopted by the SBA's Board of Directors in its resolution of 24 June 2013 and approved by FINMA on 12 July 2013. They enter into effect on 1 October 2013 and must be implemented by 30 September 2014. They replace the document of the same name which entered into effect on 1 January 2008.

Basel, 29 August 2013

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 ordinary management processes and decision-making powers.

Business Continuity Management (BCM)

Company-wide management approach (policies and standards) designed to ensure that business-critical processes 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, businesses-critical processes are continued without interruption or recovered within a defined timeframe.

Business Continuity Management Strategy

An institution uses the BCM Strategy to define its fundamental approach to Business Continuity Management. This includes the definition of a unit responsible for BCM, the definition of roles and responsibilities, and the definition of the scope of BCM activities.

A written record must be kept of decisions taken in this regard.

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 addition, Business Continuity Reporting must present the results of Business Continuity Reviews and Business Continuity Tests.

Business Continuity Tests

Regular, systematic review of Business Continuity Plans, particularly with regard to their implementation and effectiveness and up-to-dateness.

If the company has its own internal IT organisation, then the IT Disaster Recovery Plans must also be regularly tested.

Business-Critical Processes

Business processes within a company the failure of which would make 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-Critical Resources

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

Business Impact Analysis (BIA)

Identification and (quantitative and qualitative) measurement of the impact of interruptions to business activity or the loss of individual resources and/or processes. In particular, the BIA serves to identify business-critical processes and the resources required for business recovery based on an analysis of interdependencies and impact as well as an evaluation and classification of potential losses.

Business Recovery

Recovery of specific processes or business activities following an interruption to a pre-defined level or measures to be taken following a loss event (see Business Recovery Plans). Can be applied on a step-by-step basis until ordinary business activity or full capacity is restored.

Business Recovery Options

Definition of the fundamental procedure for maintaining or restoring continuous business activity in the event of a loss of critical resources (including a definition of risk acceptance, analysis of potential courses of action and fundamental decisions on the provision of replacement resources). Business Recovery Options are based on the Business Impact Analysis and form the basis for Business Recovery Plans.

Business Recovery Plan

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

Crisis

Threat situation that requires critical decisions and cannot be handled within the ordinary management structure (tools and decision-making powers).

Crisis Management Team (CMT)

Team responsible for crisis management in the event of a crisis up to the point when good working order is restored (minimising economic loss and reputational risks).

Incident

Event that results in an interruption of business activity, a loss and/or impairment of service quality, but (in contrast to a crisis) can be dealt with through the Availability Management Process.

Recovery Point Objective (RPO)

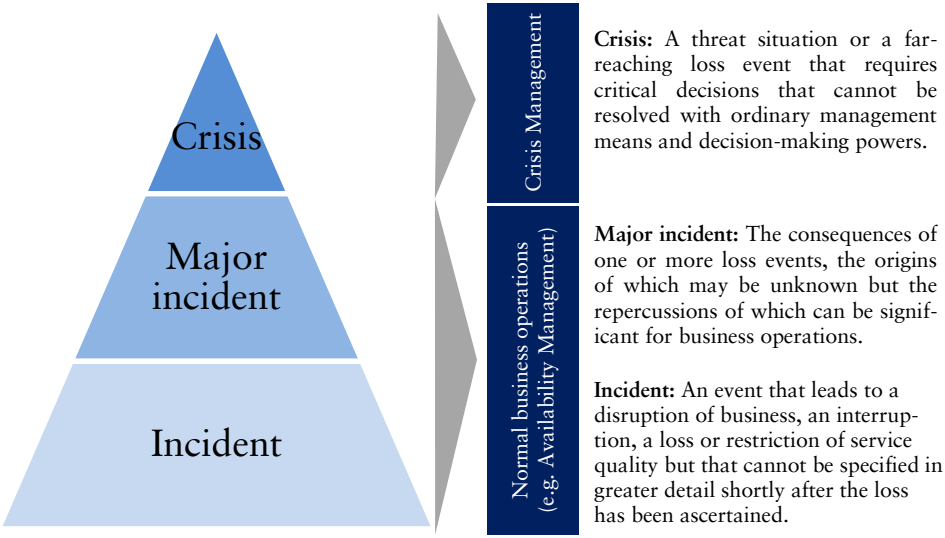
Defined, maximum acceptable data loss in the event of a crisis.

Recovery Time Objective (RTO)

Defined timeframe within which business-critical processes and/or IT services have to 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, or a crisis. Business Continuity Management is only concerned with crisis planning and crisis management.



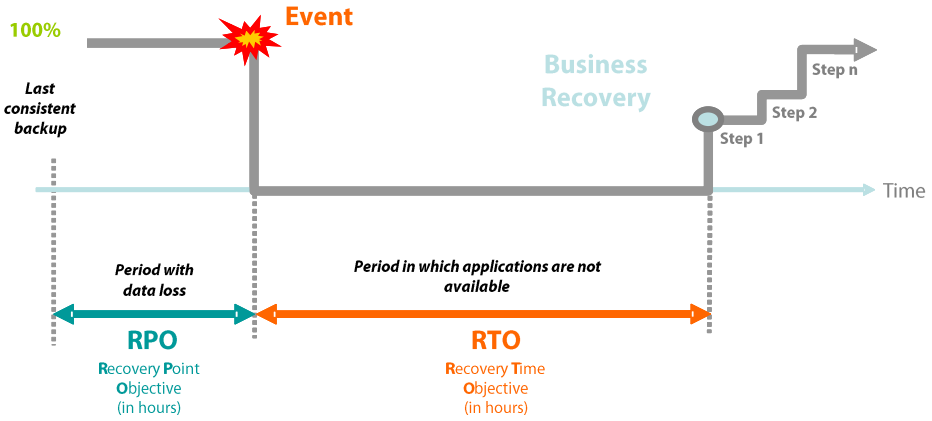
Crisis: A threat situation or a far-reaching loss event that requires critical decisions that cannot be resolved with ordinary management means and decision-making powers.

Major incident: The consequences of one or more loss events, the origins of which may be unknown but the repercussions of which can be significant for business operations.

Incident: An event that leads to a disruption of business, an interruption, a loss or restriction of service quality but that cannot be specified in greater detail shortly after the loss has been ascertained.

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 with regard to the implementation of operational Business Continuity Management processes. The list is not exhaustive.

Australian Prudential Regulatory Authority (APRA), Prudential Standard APS 232 "Business Continuity Management" and Guidance Note 232,
www.apra.gov.au

Basel Committee on Banking Supervision (BCBS), High-Level Principles for Business Continuity, Bank for International Settlements, August 2006,
www.bis.org/publ/joint17.htm

British Standards Organisation, Business Continuity Management Standard, BS 25999-2:2007,
www.bsigroup.com/en/Standards-and-Publications/

Bundesamt für Sicherheit in der Informationstechnik (BSI) (German Federal Office for Information Security), BSI standard 100-4 – Notfallmanagement (emergency management) [in German], 2008,
www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Business Continuity Institute, The BCI Good Practice Guidelines 2008 and 2010,
www.thebci.org/

Federal Reserve System (Fed), Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003,
www.federalreserve.gov

Financial Services Authority (FSA), Business Continuity Management Practice Guide, November 2006,
www.fsa.gov.uk/pubs/other/bcm_guide.pdf

Information Security Forum, Aligning Business Continuity and Information Security, March 2006,
www.securityforum.org

International Organization for Standardization (ISO), ISO/IEC 27031:2011: Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity,
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44374

International Organization for Standardization (ISO), ISO 22301:2012: Societal security – Business continuity management systems – Requirements,
www.iso.org/iso/catalogue_detail?csnumber=50038

Swiss Federal Office for Civil Protection (FOCP), Risiko- und Gefährdungsanalyse im Bevölkerungsschutz (risk and threat analysis in civil protection) [in German] March 2011,
www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/dokumente/Unterlagen_Risiken.html

Swiss Federal Office for Public Health (FOPH), Pandemic Plan – Manual for workplace preparedness, November 2007,
www.bag.admin.ch/influenza/01120/01134/03058/04319/index.html?lang=en

Swiss National Bank (SNB), Business continuity in the Swiss financial sector, January 2006 and September 2009,
www.snb.ch/en/iabout/finstab/id/finstab_bcp

Swiss Bankers Association
Aeschenplatz 7
PO Box 4182
4002 Basel
Switzerland
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org