Business continuity planning in the Swiss financial centre
Review of the current situation

BCP steering committee for the Swiss financial centre

September 2009

Executive Summary

In its report published in 2006, *Business Continuity Planning in the Swiss Financial Centre*, the business continuity planning steering committee (BCPsc) assessed contingency planning in the area of operational risks and proposed various measures to improve the situation, both at individual financial institutions and in the financial centre as a whole. The analysis upon which the report was based focused on two business processes which were judged to be particularly critical in ensuring financial stability. These were large-value payment transactions between financial institutions and the supply of liquidity to the banking system by the Swiss National Bank (SNB). In this review of the current situation, the BCPsc aims to provide information on the most important achievements since the 2006 Report was published as well as areas where more action is needed.

Over the last few years, the institutions represented in the BCPsc have adopted a variety of measures to further increase their operational resilience in the event of a crisis. Test results show, for instance, that the operators of key financial market infrastructure are in a position to restore processing of critical business transactions within two hours, even after a major disruption has occurred, and critical system participants will be operational within a maximum downtime of four hours. Moreover, in the area of key infrastructure, the opening of a third, out-of-region data centre has significantly increased the level of resilience in the event of a disaster affecting a large geographical area. In addition, all institutions have drawn up plans and measures whereby their critical business processes can be maintained even if a significant proportion of the staff required for such processes in normal operations are unable to work.

Alongside measures specific to individual institutions, various industry-wide measures have been implemented over the past few years that have required a coordinated approach by the individual institutions. For instance, an industry-wide alarm and crisis organisation has been instituted, in which the key market participants and the most important providers of infrastructure services are represented. In the future, the BCPsc intends to conduct more scenario-based emergency trials with representatives of the alarm and crisis organisations. These will focus on coordination and decision-making in crisis situations. In addition, the SNB and SIX Interbank Clearing Ltd have concluded an agreement which provides for SIX Interbank Clearing Ltd to take on certain operational functions normally carried out by the SNB, if necessary.

As a result of these measures, the level of preparations in the area of operational risks has risen even higher in the last few years than that achieved in 2006 (which was already good). For the near future, the BCPsc plans to further intensify its cooperation with other sectors that provide critical services to the financial industry. It will also evaluate any possible need for action in additional business processes such as, for example, retail payment transactions.

1. Introduction

In February 2006, the business continuity planning steering committee (BCPsc), a group organised by the Swiss financial centre, published its report, *Business Continuity Planning in the Swiss Financial Centre* (hereafter referred to as the 2006 Report). The BCPsc is made up of representatives of the authorities (Federal Financial Market Supervisory Authority, FINMA; Swiss National Bank, SNB), the financial institutions (Citigroup, Credit Suisse, PostFinance and UBS) and the financial market infrastructure operator SIX Group (including subsidiaries). The main aims of the BCPsc are to coordinate the contingency planning and management efforts of the individual institutions in the area of operational risk and to strengthen the operational resilience of the Swiss financial centre. In this way, the BCPsc makes a contribution to the stability of the Swiss financial system.

The 2006 Report focused on business processes that were classified as particularly critical in terms of financial stability. It assessed business continuity planning in the Swiss financial industry and identified a number of ways in which it could be improved. Measures to be taken should, in particular, ensure that a major disruption to the processing of critical business transactions does not affect the entire financial system and threaten its stability.[1]

Since the 2006 Report was published, the institutions represented in the BCPsc have evaluated the proposed measures and implemented most of them. In this review of the current situation, the BCPsc provides information on the most important achievements since the Report was published and on the areas where more action is needed. The information provided in sections 3 and 4 of this review is partially based on statements made by experts from the institutions represented in the BCPsc. In early 2009, these experts were interviewed in depth by the SNB on the current state of internal and industry-wide contingency planning and management measures.

2. Recommendations of the 2006 Report

The 2006 Report assessed the level of business continuity planning in the Swiss financial industry and proposed various measures for improving contingency planning and management in individual financial institutions and in the financial centre as a whole. The analysis upon which the Report was based focused on two business processes which were judged to be particularly critical in ensuring financial stability. These were large-value payment transactions between financial institutions and the supply of liquidity to the banking system by the SNB.

In the 2006 Report, the BCPsc noted that good contingency measures had already been put in place by the institutions represented on the committee. To ensure that these measures could actually be implemented when needed and that procedures could be coordinated even in unexpected situations, the BCPsc planned to integrate the provisions made by individual

[1] The 2006 Report can be accessed on the Swiss National Bank website (www.snb.ch).

institutions within an overall framework. The 2006 Report therefore drew up requirements on, in particular, the maximum downtime for financial market infrastructures and critical system participants. Operators of key infrastructure must be able to restore processing of critical business transactions within two hours, even after a major disruption; the corresponding period for critical system participants is four hours.

In addition, the 2006 Report proposed further measures, some of which can be implemented by the individual institutions and some of which also require coordination between the institutions. The recommendations made to the individual institutions can be summarised as follows:

- Creating conditions that allow for critical business processes to be restored within the specified time period, either through the use of alternative processes or through the restoration of normal processes;
- Reviewing the physical distance between the locations of the main data centres and the back up data centres;
- Giving greater consideration in the contingency measures to the consequences of staff being unable to work.

The most important industry-wide recommendations were:

- Establishing an industry-wide alarm and crisis organisation;
- Reviewing the possibility, in exceptional situations, of calling a bank holiday at short notice in the SIC large-value payment system;
- Reviewing the extent to which the SNB and SIC Ltd, which operates the SIC large-value payment system on behalf of the SNB, can act on behalf of one another in exceptional situations;
- Intensifying contacts with the telecommunications industry.

The two sections that follow provide information about the most important progress with regard to operational resilience in the Swiss financial centre since the 2006 Report was published, and about the current level of implementation of the measures outlined above in individual institutions and within the financial centre as a whole.

3. Level of implementation of institution-specific recommendations

Over the last few years, the institutions represented in the BCPsc have adopted a variety of measures to further increase their operational resilience in the event of a crisis. The institutions' main focus has been, first, on investing in existing or new technological equipment and premises, and, second, on adopting organisational measures to ensure greater preparedness against any loss of staff. Besides the findings of the 2006 Report, the Swiss Bankers Association's *Recommendations for Business Continuity Management (BCM)*,

published in November 2007, provided a major impetus to these efforts. These recommendations, which are aimed at all banks in Switzerland, are in principle not binding – with two important exceptions. As of the end of 2009, FINMA will require banks and securities dealers, first, to carry out a business impact survey and, second, to define a business continuity strategy, as a mandatory regulatory minimum standard.

The principal requirement laid down in the 2006 Report is that operators of key financial market infrastructure must be able to restore critical business processes within two hours, even after a major disruption; for critical system participants, the **maximum downtime** is four hours. The Report mentioned that system participants could fulfil this requirement by changing over to alternative processes. However, discussions held in the meantime have revealed that the practical obstacles to implementation of effective alternative processes, in particular as regards large-value payments, are prohibitively high. This therefore only leaves the option of creating the technical and organisational prerequisites for normal processes to be restored within the prescribed period. The individual institutions have aligned their business continuity plans for critical business processes with these requirements, and test them regularly. The test results show that both the operators of key infrastructure and the critical system participants are able to meet the requirements.

In this connection, it should also be noted that, overall, both the scale and the frequency of **tests and exercises** have continued to increase over the last few years. Such tests and exercises are aimed at identifying whether the BCP drawn up for specific institutions can be implemented in a crisis as planned, and whether the prescribed timetable can be adhered to. All institutions regularly test their BCPs for restoring identified critical processes, including the necessary resources. In addition, all institutions have their own crisis teams, with clear division of responsibilities and competencies.

The 2006 Report highlighted the **distance between the main and backup data centres**, which was fairly short by international standards, and could have adverse consequences in the event of a major incident affecting a wide geographical area. As regards the central financial market infrastructures (i.e. the large-value payment system SIC and the securities clearing system SECOM, which are both operated by subsidiaries of SIX Group), this risk has since been reduced considerably through the establishment of an additional out-of-region data centre. Another financial institution has set up a new, geographically separate backup data centre.

Moreover, a comparison with the situation of a few years ago shows that the individual institutions are now substantially better prepared against the **loss of staff**. All institutions have drawn up plans and contingencies to ensure that critical business processes can be maintained even if a significant proportion of the staff required for such processes in normal times are unable to work. A typical measure is to make sure that staff are trained to work in a number of different areas. Furthermore, through the introduction or more systematic use of shift work, right up to the permanent geographical dispersal of individual departments as part of normal operations, it can be ensured that not all staff employed in a critical function

are affected by an operating incident at one business location. Finally, precautions have been taken to ensure that critical functions are also maintained when staff are unable to reach a given location. These include, for instance, providing backup workplaces for particularly important activities and encouraging home working. There is, however, no 'one size fits all' solution; the suitability of organisational measures depends heavily on the institution's situation. Moreover, certain organisational measures bring their own challenges, both for staff and, in particular, for managements.

The latent threat of a pandemic is one of the reasons for having paid increased attention to precautions with regard to the possible loss of critical staff members. For a **pandemic scenario**, the institutions have introduced a number of specific measures, ranging from providing medical advice and laying in stocks of essential equipment (protective face-masks, disinfectant, medication, food, etc.) to drawing up specific contracts with external service providers and making it possible for staff to work from home. As regards this last point, not all institutions are adopting the same strategy, not least because it is unclear whether, in the event of a pandemic, the risk of infection is greater at home or at work.

4. Level of implementation of industry-wide recommendations

In addition to the measures which individual institutions can take themselves, the BCPsc is also concentrating its efforts on aspects which can only be implemented in an industry-wide context. The 2006 Report therefore also contains a number of recommendations whose implementation requires a coordinated approach that has been agreed between the individual institutions.

Before the 2006 Report was even published, an **industry-wide alarm and crisis organisation** was instituted, in which the key market participants and the most important providers of infrastructure services are represented. The heads of BCM from the participating institutions make up the top level of this crisis organisation, with the lower levels forming a network between those responsible for the areas of liquidity, large-value payments (SIC), retail payment transactions and IT. Any of the institutions can invoke the alarm organisation by activating the level affected. The institutions involved in the alarm and crisis organisation rate it positively overall, based on their experiences, but have identified a need for improvement with regard to the frequency and mandatory nature of alarm tests. Moreover, the alarm and crisis organisation needs to be more firmly anchored at some levels.

As well as the alarm tests carried out to date, the BCPsc also plans to perform an increased number of **scenario-based crisis exercises**. These exercises are aimed at strengthening the communication, coordination and decision-making of participants in the event of a crisis. The first industry-wide crisis exercise is currently at the planning stage, and should take place in the course of this year.

The 2006 Report also advocated an investigation into whether, in the event of a major operational disruption, it would be possible to declare a **bank holiday** for the SIC payment system at short notice, and thereby win time in which to solve the problem. Investigations revealed that such a move would face considerable practical obstacles, as well as legal problems.

A further recommendation was to check the extent to which institutions can provide **reciprocal support** in the event of a crisis. As a specific measure, the SNB and SIX Interbank Clearing Ltd have concluded an agreement which provides for SIX Interbank Clearing Ltd to take on certain operational functions normally carried out by the SNB, if necessary.

In addition, **contacts with the telecommunications industry** have been strengthened – as suggested in the 2006 Report. Joint efforts are underway to check the availability of critical telecommunications services for the financial industry in the event of a crisis, and identify joint measures to be taken where necessary.

5. Outlook

This review of business continuity planning in the Swiss financial industry shows that the measures detailed in the 2006 Report have largely been implemented. The level of preparations in the area of operational risks has risen even higher in the last few years than that achieved in 2006 (which was already good).

For the near future, the BCPsc intends to intensify the joint efforts already begun with the telecommunications industry. In addition, it hopes that the scenario-based crisis exercise planned for later this year will yield further insights into BCP coordination requirements. The BCPsc also plans to assess the extent to which there is a need for joint efforts to strengthen the operational resilience of other business processes – for example, retail payments.

Given the constantly evolving threat scenarios, it is very important not to relax efforts to maintain and improve operational resilience. For instance, in recent years the pandemic threat has attracted increasing attention and made new measures necessary. In the future, too, steps must be taken to ensure that the financial industry follows such developments closely, to enable it to take appropriate and timely action. Finally, in the view of the BCPsc it is essential that business continuity planning at individual institutions continues to receive appropriate attention, even during periods of heightened cost pressure.