Business Continuity Planning in the Swiss Financial Centre

A Joint Paper by an Industry Group of the Swiss Financial Centre

January 2006

Business Continuity Planning in the Swiss Financial Centre – List of Contents

For further information contact:

Daniel Heller, Director, Financial Stability and Oversight, Swiss National Bank
(+41 44 631 37 26)

1. Introduction and Management Summary

The stakeholders of the Swiss Financial Centre[1] decided in 2004 to undertake a stock taking exercise of the general state of preparation for business continuity provisions in the financial system in Switzerland. Gaps and possibilities for improvement were to be identified and suggestions for improvements to be brought forward. This paper provides a summary of the results.

The objective of the analysis is to ensure financial stability in Switzerland in the event of an exceptional incident. The analysis is focussed on financial stability and is therefore restricted to activities in the wholesale financial markets in Switzerland. Activities solely related to financial services in the retail sector are not included.

In the course of the analysis, the following working steps were completed:

- Identification of the business areas within the wholesale financial markets that are critical from a systemic point-of-view: Settlement of large value payments via Swiss Interbank Clearing SIC and liquidity provision via repo;
- Definition of events ('disaster scenarios') that should be covered: Physical loss of any key building with all employees working there;
- Grouping of all institutions involved: Market infrastructures comprising the central accounting infrastructure at the Swiss National Bank, automated repo trading system at Eurex/Swiss Exchange SWX, securities settlement system SECOM/SIS at SegaInterSettle, payment settlement system Swiss Interbank Clearing SIC/Telekurs on the one hand and important participants on the other;
- Assessment of the BCP provisions currently implemented at each identified institution;
- Working out of guiding principles applicable to business continuity planning in the wholesale Swiss Financial Market;
- Setting up of an inter-institutional alarm and crisis organisation for the financial market place as a whole;
- Identification of further improvements.

As a general objective the requirement was defined that the systemically essential market infrastructures should recover within a two hour framework in the event of an exceptional incident and that important participants in such infrastructures should resume processing of critical business transactions within four hours. This general objective also matches requirements set up internationally in other markets.

On the whole, a good state of preparation has been identified for all institutions involved in the working group. Possibilities for further improvement have been identified and will be implemented over time.

A set of four guiding principles for business continuity planning were defined and three projects for further improvement identified. In addition, as an immediate measure, an inter-institutional alarm and crisis organisation was set up.

The normative basis for the implementation of the agreed standards shall be provided by relying on the existing ordinance issued by the Swiss National Bank, applying both a direct

[1] Swiss National Bank SNB, Swiss Federal Banking Commission SFBC, Credit Suisse, UBS, PostFinance, SIS Group, Swiss Exchange SWX, Telekurs Group

and an indirect approach: The Swiss National Bank SNB agrees with system operators conditions that are subsequently implemented by these system operators for themselves and, where applicable, included in the rules for their system participants.

In addition, contacts with the communication sector shall be intensified, as this sector plays a key role in all BCP preparations of the financial markets. This can be done within the Swiss national crisis precaution activities.

2. General Objectives for Business Continuity Planning

The financial system operates in a network of interrelated markets, market infrastructures and participants. The functioning of any individual link in this network can have effects beyond its own operations, affect other institutions in the network and lead to wide-ranging disruption for the financial system as a whole with impact on the entire economy. Because of this interdependence within the financial system and the importance for the entire economy, every institution in the network has a role to play to ensure resilience of the system as a whole. At the same time, a balance must be struck between the risks posed and the costs related to any preparatory measures.

For the purposes of this report, the following methodical notion is used for the term Business Continuity Planning:

1. Preventive measures taken in anticipation of a disruption to avoid it happening at all, such as physical guards, firewalls etc.;

2. Precautionary measures taken in anticipation of a disruption to cope with the effects once an incident has happened, with the objective to
    a. rapidly take up normal standard procedures again (e.g. on back-up systems);
    b. temporarily use alternative procedures that can be applied without relying on IT applications usually used in day-to-day processing to cope with the most important business transactions during a transition period.

The overall resilience of the Swiss financial system in the event of any type of disruption must meet the following general objectives:

- Avoidance that a disruption of processing for business areas identified as critical has an impact on the financial system as a whole

  This objective is achieved either by the timely resumption of such processing at the affected institution based on the usual operational infrastructure or by switching to alternative processes that offer an interim solution;

- Maintaining a high level of confidence that the business continuity arrangements are effective

  Regular use (‘training and test’) of identified alternative arrangements and back-up procedures ensures that such provisions remain operational and maintain a high level of credibility;

- Ø Ensuring a level of preparation that allows a coordinated approach in case of any disruption ('prepare for the unexpected')

  A sound alarm and crisis organisation on the inter-institutional level that can be called upon fast and at any time ensures that a framework exists to coordinate all activities in the emergence of any kind of disruption. The crisis organisation must also be subject to regular use by making it subject to training exercises.

The provisions in this paper cover activities in wholesale financial markets in Switzerland. Financial stability is the primary focus. For this reason, solely business areas in the Swiss wholesale financial markets have been investigated. Definitions and priorities have been set up accordingly. Other activities such as retail financial services are not part of this report although they also may be important for the economy as a whole and for the population in general.

3. Definitions

Business Continuity is a broad topic. Definitions and the setting of priorities are therefore indispensable. To ensure a high level of confidence, full transparency of these definitions, their criteria and the priorities derived is essential.

In the course of this study, definitions for the following points were investigated:

- Business Processes
- Business Functions
- Scenarios of Events
- Business Units

3.1 Business Processes

The following business processes were identified as core for the wholesale Swiss financial markets from a financial stability point-of-view:

- Large value payments via the Swiss Interbank Clearing SIC ('financial payments') and
- Liquidity provision via the repo market.

These two business processes are essential to allow for a sufficient level of activity in the Swiss financial markets.

A generally accepted definition for the term 'large value payment' is not available[2,3]. The assessment of a payment as 'large value' is something relative and depends for example on the size of the institution(s) involved in the payment transaction (effect on liquidity). An

[2] The BIS report ‚A glossary of terms used in payments and settlement systems' defines 'large value payments' as 'payments, generally of a very large nature, which are mainly exchanged between banks or between participants in the financial markets and usually require urgent and timely settlement' which does not allow for a precise distinction for BCP purposes.

[3] When the Swiss Interbank Clearing SIC went live more than 15 years ago, all participants had to process payments as from a threshold of CHF 1 million mandatorily via SIC to ensure a smooth flow of liquidity in the settlement system.

analysis of payment values in SIC is contained in the appendix to this report. From the figures shown, a limit of either CHF 1 million or 5 million is justified.

More importantly, also some payments of a lower value such as pay-ins for CLS Bank must be regarded as very urgent and important. It is therefore indispensable that a participant ensures processing of payments in case of a disaster in an order of priority (processing the most urgent payments first). The value of an individual payment is only one aspect to be taken into account when setting priorities.

For BCP from the point-of-view of financial stability, retail payments (including debit and credit cards), the provision of cash (banknotes) and securities trading are only of secondary importance. However, measures suggested in this report also improve the situation in the field of retail payments (e.g. alarm and crisis organisation, availability of Swiss Interbank Clearing SIC as SIC also processes large volumes of retail payments). Experience in other disaster situations has shown that it is correct to regard securities trading as of secondary importance – securities markets were on occasion even closed deliberately until the situation in the financial markets had stabilised.

3.2 Business Functions

It is indispensable that all business functions needed for the operation of the business processes identified as critical are available.

When investigating the level of preparation in individual institutions, the following business functions were specifically analysed:

- IT
  - Physical infrastructure such as data centres, software etc.;
  - Staff resources for IT processing;

- Business
  - Physical infrastructure for business operations such as offices, work stations etc.;
  - Staff resources for business processing.

3.3 Scenarios of Events

The working group analysed and categorised possible events as follows:

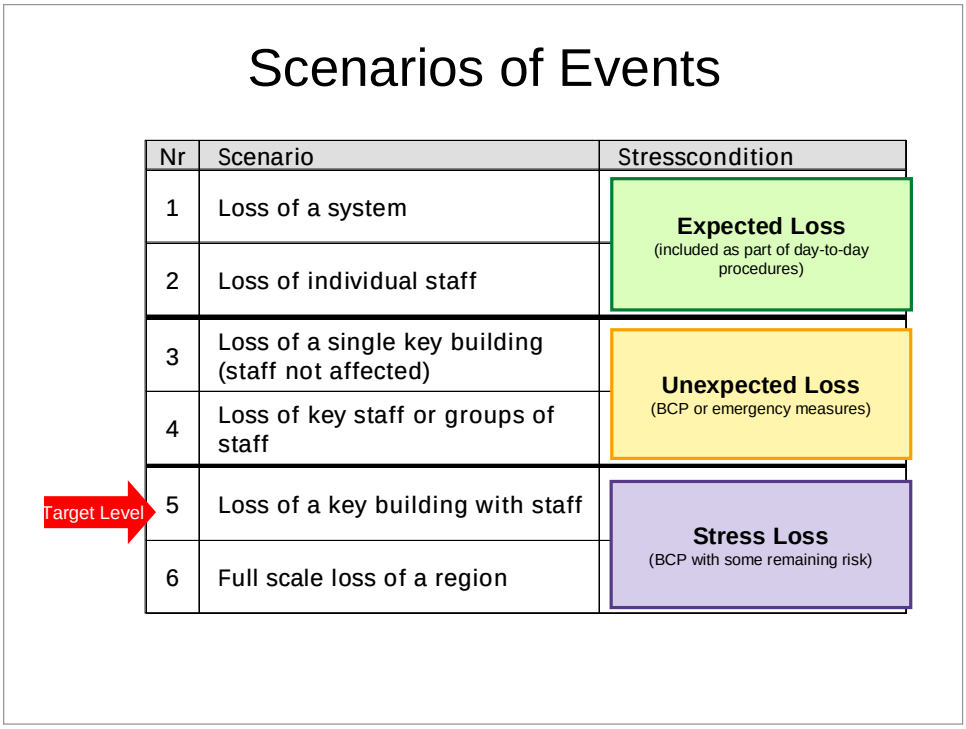

Illustration 1: Scenarios of Events

Broad consensus exists that the analysis for BCP in the Swiss financial market shall concentrate on level 5 in above illustration, the loss of any key building including the staff working in this building. Levels 1 to 4 in above illustration must be covered by each individual institution. They are implicitly contained in any precautionary measures for level 5.

The reason why a key building (technical fault, accident, terrorist attack, natural disaster, quarantine because of an epidemic incident etc.) is lost is irrelevant. By concentrating on level 5 of above scenarios of events, multiple events affecting multiple sites are excluded. However, sound preparations for level 5 by all institutions involved implicitly also contribute to overcome such multiple events.

In this respect, problems regarding system or application software as well as data management systems represent a speciality. They are contained in level 1 and must therefore be covered by each individual institution. A problem in any of these fields will usually affect at the same time both the primary and the secondary site of the institution involved as they both operate on the basis of the identical software and identical data. Such situations can occur suddenly or slowly arise over several days. In the current environment, the likelihood of such an event must be regarded as higher than that of many purely physical disasters, for which extensive preparations have been made. At the same time, precautionary measures to cope with such an event, e.g. by providing for a complete set of alternative system and application software, are extremely difficult and very costly to implement. Preventive measures are therefore of primary importance in this respect.

3.4 Business Units

For purposes of this analysis, institutions involved are grouped into

- central infrastructures (market infrastructures) and
- participating institutions (important participants).

For institutions in these two groups, differing requirements for coping with exceptional situations may be justified, especially with regard to maximum down times. In general, the requirements for central infrastructures will be higher than for participants. At the same time, the requirements for important participants will be higher than for other participants.

Central infrastructures involved in the processing of the identified critical business processes are

- the Swiss National Bank SNB: Provider of liquidity and operator of settlement accounts;
- Eurex/SWX: Repo trading;
- SECOM/SIS: Repo settlement;
- SIC/Telekurs: Payment settlement.

For important participants the question arises how to define them objectively. Usually, the share in the value or volume processed in the central infrastructure is used for this purpose. Shares between 5% and 20% are used to classify a participant as important. Applying these thresholds in Switzerland would lead to the following number of participants being regarded as important:

Business Process	Number of Important Participants	
	20%	5%
Large value payments	1-2	3-4
Liquidity provision/Repo	1-2	5-6[4]

It is difficult to simply apply market share thresholds used abroad to define important participants in central infrastructures in Switzerland. An analytically correct and objectively justifiable threshold can really only be found by carrying out a full-blown simulation: Which participants are indispensable to ensure a smooth operation of the central infrastructure?

On the other hand, volume or value share of each individual participant may also be misleading. Some participants in central infrastructures make use of shared utilities or use the same provider to connect to the central infrastructure. Such combinations may lead to a situation where institutions that individually are not regarded as important may, on a combined basis, reach the threshold. It was decided to include such combinations when defining important participants in central infrastructures.

[4] 1 or 2 of which domiciled outside Switzerland

4. Existing Rules and Precautionary Measures

The working group included in its analysis existing rules and precautionary measures, both on an international and on a national level.

On the international level, the primary focus was on the Interagency White Paper published by the US regulatory authorities.

Domestically, the new National Bank Law, transferring to the Swiss National Bank SNB an oversight role over settlement systems and the ordinance issued by the SNB setting down minimum requirements for systemically critical settlement infrastructures provide a basis for BCP. The ordinance determines that an operator of a critical market infrastructure meets high requirements with regard to reliability, integrity, confidentiality as well as internal controls and that recognised security standards must be complied with. The detailed policy of the SNB for implementation of its new powers is not yet fully known. The critical settlement infrastructures for purposes of the SNB ordinance have been defined (SIC, SIS x-clear, SIS SegaInterSettle and CLS Bank). The oversight role of the SNB is limited by law to settlement systems and does not comprise trading systems.

In addition, there are requirements defined by the Swiss Federal Banking Commission SFBC applicable to all institutions it regulates (banks, securities traders). These requirements do not explicitly mention business continuity. But this must be regarded as included in the term of 'orderly conduct of business' that applies to all regulated institutions. In the context of the year 2000 preparations, the SFBC issued a circular that required banks to explicitly set up a contingency plan. The SFBC expects that institutions it regulates did not set up a contingency plan solely geared to one single event, but on a more general basis, and that they regularly update this plan.

Switzerland has also developed a comprehensive organisational basis to cope with all sorts of extreme incidents ('Wirtschaftliche Landesversorgung WL', economic provisioning of the country). WL is responsible for the provisioning of the country with all indispensable goods and infrastructures in case of a crisis of any sort. In this respect, the communications sector is of particular importance for the financial sector. Whereas other supplies such as electricity, water etc. can be secured by financial institutions for a limited period of time on an individual basis (electricity, for example, by having diesel power generators available), dependence on the telecommunications infrastructure is unavoidable. Communication is also necessary for the processing of the identified critical business processes.

Authority in this respect is provided by two articles in the Swiss constitution (Art. 102 on supplies for the country and Art. 185 on external and internal security). Art. 185 is of particular importance for a situation of crisis, as it gives the Swiss Federal Council in such a situation the power to directly issue decrees. Based on this article of the constitution, power can also be given to other competent authorities to urgently overcome difficult situations. But such powers can only be expected to be used in very extreme situations.

5. Results and Recommendations

The working group conducted a detailed analysis of the existing precautionary measures at individual institutions.

Overall, the working group came to the conclusion that the level of preparation at the individual institution is good. However, it was regarded as worthwhile to bring the preparations into an overall framework of guiding principles that was not yet available.

5.1 Basic Requirement for Maximum Downtime

The basic requirement for central infrastructures and participants can be summarised in the following overview:

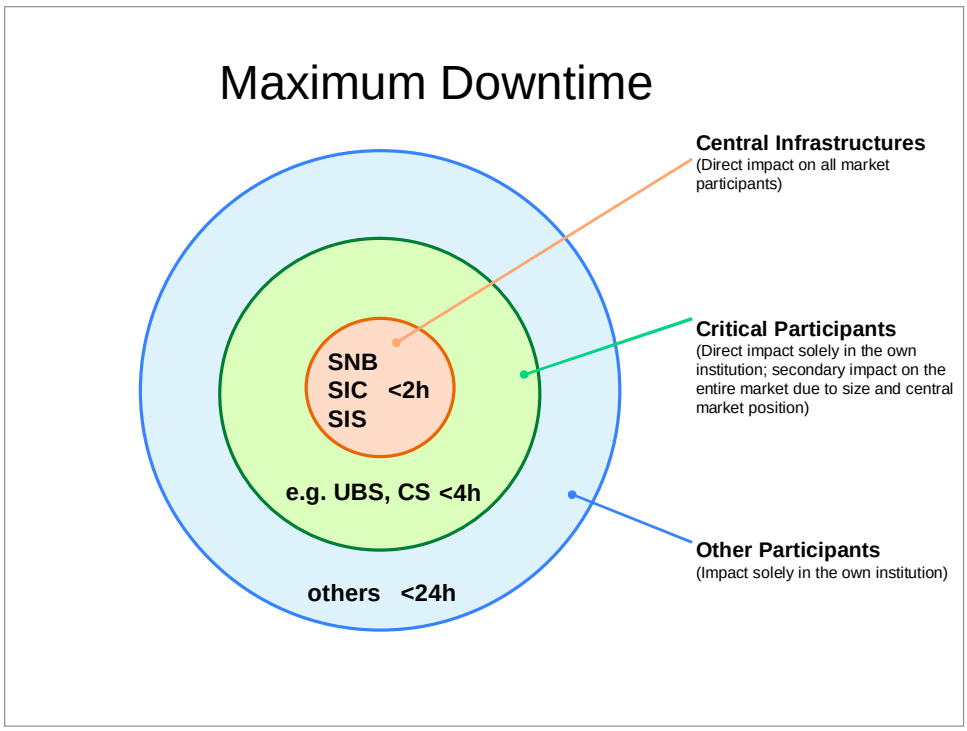

Illustration 2: Maximum Downtime

As a guideline, central infrastructures should resume processing of identified critical business processes in the event of an incident affecting any key building of theirs within a timeframe of two hours. For important system participants this maximum downtime for the processing of identified critical business processes is four hours. For all other participants, as far as they are subject to regulation under the Swiss Banking Law, the requirements of the Swiss Federal Banking Commission SFBC are applicable. Precautionary measures of central infrastructures and participants must be geared towards usually meeting these guidelines. The basic requirement follows closely the ones set up in the US Interagency White Paper.

5.2 Assessments and Observations

The analysis of the working group led to a number of assessments:

- On the whole, preparations of market infrastructures and important participants can be regarded as good.

- The distance between primary and secondary sites are frequently, measured by international trends, below average.
  In this respect, three points need to be taken into account:
  - Distance as such cannot be regarded as the sole criterion for assessment. The Swiss National Bank in its ordinance takes this point up by stipulating that two sites must be subject to different risk profiles.
  - For data centres, a careful consideration must be made between distance and quality (availability of fully up-to-date data, loss of data, good availability in day-to-day problem management).
  - While technical possibilities are increasing over time, investment cycles must also be taken into account. Introducing every new possibility that becomes technically available would lead to huge ongoing investments ('every two years a new data centre 20 kilometres further away') which is not viable.

  The requirements, as far as distance between primary and secondary sites is concerned, need to be followed on an on-going basis and include an assessment of possible future threats.

- Tests in the IT environment hitherto were usually done on a prepared basis to avoid risks in day-to-day processing created by the disaster recovery test. It is important to continually improve the test environment so that tests can be conducted on a basis as near to reality as possible without creating new risks to day-to-day processing resulting from the test itself.

- Precautionary measures at individual institutions are usually better geared towards the loss of physical components (hardware, building) than towards the loss of staff.

- As soon as buildings are used in a 'multifunctional way' (data centre, IT staff and business staff in the same building), this accumulation leads to additional risks in case of an extreme disaster that need to be taken into account.

- No benchmark, applicable to the specific situation and market structure in Switzerland, has been developed to determine which participants are to be regarded as 'critical' for the system as a whole.
  By making use of alternative processes for the identified critical business processes by all major participants and by setting up by the central infrastructures facilities to support medium-sized and smaller institutions to also make use of such alternative processes, defining exactly which participants must be regarded as critical becomes less important.

In addition, the following observations need to be made:

- Taking into account the actual threats, the question arises whether preparations for problems with system or application software as well as data management systems are taken into account sufficiently. Problems in these areas must be regarded as more probable than some physical incidents for which preparations exist.

With the exception of SIC, in this field reliance on preventive measure dominates and precautionary measures are rare. With regard to MiniSIC the question must also be asked whether its batch processing can really fully meet today's requirements (timed payments for CLS Bank, remote participants in SIC). On the other hand, batch processing in MiniSIC in case of an incident affecting SIC will be sufficient for most retail payments settled via SIC today.

- In exceptional situations it may be useful to 'buy time' by declaring a business day at short notice to a bank holiday in SIC. The implications of such a step are today not known, neither on the legal nor on the operational level (payments in the forward value transaction data file etc.).

5.3 Conclusions and Guiding Principles

The following conclusions and guiding principles have been accepted:

1. The central infrastructures needed for the processing of the identified critical business processes at the Swiss National Bank SNB (for repo trading and for account entries/system monitoring regarding Swiss Interbank Clearing SIC), at Telekurs (for SIC) and at SIS SegaInterSettle (for SECOM/Repo) must meet very high standards with regard to short downtimes without loss of any data relating to confirmed transactions. As a guideline, the maximum downtime should not exceed two hours. This applies to all sorts of disastrous event.

   Justification: There are no alternatives for these central infrastructures (in this respect, MiniSIC, too, does not provide an alternative for the identified critical business processes). The loss of these central infrastructures would lead to a de facto standstill of the Swiss financial market.

2. High standards shall also be applicable for important participants. They shall resume processing of the identified critical business processes within four hours.

   How important participants meet this requirement is left to them to decide. Their options are to either resume processing within this deadline making use of their usual operational infrastructure or by switching to alternative processes that offer an interim solution.

   Even when deciding to make use of alternative processes, the requirements to resume processing based on the usual operational infrastructure remain high as alternative processes can only offer an interim solution. To make use of alternative processes in case of a disaster also requires comprehensive preparations (e.g. availability of customer orders and business operations).

   Justification: Without the availability of (important) participants the precautionary measures taken at the level of central infrastructures are of limited value.
   Making use of alternative processes that are available for an interim time after a disaster and allow for the processing of a limited number of particularly important transactions, provides for the following reasons a very strong security network:

   a. Alternative processes can be made available by/for all important participants, not just for the ones that are regarded as particularly critical. Shifts in market structure

that can occur at very short notice and lead to further participants becoming critical from a systemic point-of-view, can therefore be taken into account instantly and much more easily.

b. The switch to alternative processes can be made fast and irrespective of the root cause of a disaster. A switch can take place even within a shorter timeframe than within four hours as both the switching to the alternative process and the switching back to the normal operational infrastructure do not require much instant preparation (e.g. after a loss of the data centre just before the close of CLS Bank settlement, some timed CLS payments can be made via the alternative process while investigation of the cause in the data centre has only just started). The ease of switch in both directions makes the decision to initiate such a switch also much easier.

c. Alternative processes are available irrespective of the root cause of the problem. Especially, alternative processes are available also in the case of system or application software problems or problems with data management systems (that affect both the primary and the secondary data centre).

The prerequisites to make systematically use of alternative processes at a reasonable cost are favourable. Some, including the two largest, participants already have equipment available to implement alternative processes in case of an incident occurring. For other (important) participants, the transaction volumes of which are already considerably smaller, the necessary infrastructure could be provided by the central infrastructures on the basis of an 'acting-on-behalf-of' arrangement.

3. Repo trading on the platform of SWX/Eurex can be made subject to less stringent requirements, as an alternative process has already been defined that can be implemented at short notice to transact the most important repo financing transactions.

   Justification: This alternative process offers an option that covers far reaching disaster scenarios.

4. Preventive measures against disruptions caused by system or application software as well as data management systems are of particular importance for the central infrastructures at the Swiss National Bank SNB, Telekurs/SIC and SIS/SECOM. The preventive measures at these institutions must be subject to continuous review with the objective to keep them at the highest level possible.

   Justification: These central infrastructures are of core importance and alternatives to their services are only very limited.

   In addition, possibilities should be analysed how, within the day-to-day distribution of functionality between the systems operated by the Swiss National Bank SNB and Swiss Interbank Clearing SIC, one system can take up some tasks in case of a disruption of the other system to ensure limited continuation of processing (e.g., in case of a loss of SIC, acceptance and processing of large value payments sent by participants via SWIFT to the Swiss National Bank within the banking application operated by the SNB, or, in case of a loss of the SNB system, carrying forward of end-of-day balances within SIC to the next business day).

5.4 Interbank Alarm and Crisis Organisation

Inevitably, preparatory and precautionary measures can never completely include all incidents as they will occur in reality. There will always be events that are beyond initial imagination. It is therefore important to create structures that can cater for the unexpected and remain flexible to adapt to the events as they occur in reality.
In such a case, all affected institutions must be in a position to get in contact with each other very fast and coordinate necessary actions.

The working group therefore decided to set up an alarm and crisis organisation on an inter-institutional level. This alarm and crisis organisation is available to discuss matters beyond the critical business processes identified in this report and to take the necessary decisions:

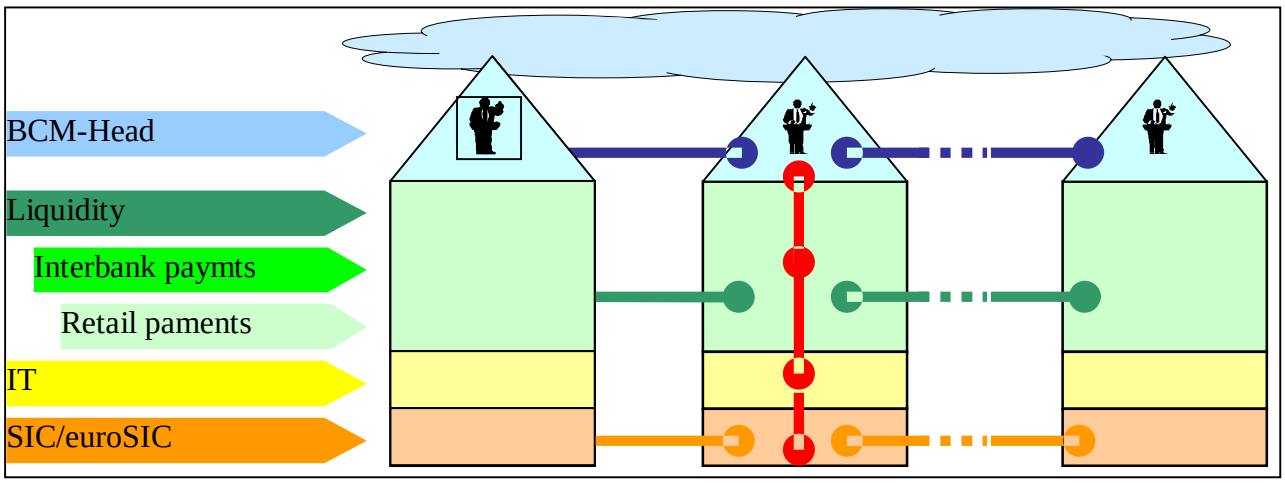

Illustration 3: Interbank Alarm and Crisis Organisation

The highest level of the interbank alarm and crisis organisation consists of one responsible person from the BCP organisation of the institutions involved. On the lower levels (liquidity, payments, SIC), individuals are also nominated by each organisation. They provide for a communication platform when more detailed problem and process related knowledge is needed. In case of an interruption, any institution can invoke the alarm organisation. This institution also takes the initial lead in the crisis organisation until an alternative lead is agreed on. Each institution remains responsible for its own preventive and precautionary measures as well as for managing the interruption within its own institution. As soon as the alarm organisation has been invoked and as long as it remains in force, external communication will also be coordinated within this crisis organisation. The alarm and crisis organisation will be subject to regular (yearly) test and training.

6. Next Steps and Implementation

Each institution remains responsible to implement measures identified within its own institution. On an inter-institutional level, the following projects have been identified:

- Detailed agreement on the preparations for the proposed overall BCP solution including creating the prerequisites for alternative processes and an 'acting on behalf of' (responsibility: existing interbank working group PAP) as well as the identification of important participants in market infrastructures (responsibility: Swiss National Bank SNB)[5];

- Assessing feasibility to finding of a way to declare a 'short notice bank holiday' in the Swiss Interbank Clearing SIC (responsibility PAP; to discuss legal matters, a mixed group of representatives from legal departments under the lead of a representative from a bank will be set up);

- Analysis of possibilities, within the day-to-day distribution of functionality between the systems operated by the Swiss National Bank SNB and Swiss Interbank Clearing SIC, to ensure that one system can take up in case of a disruption of the other system some disrupted functionality to ensure limited continuation of processing (responsibility Swiss National Bank SNB in coordination with PAP).

  Within each above mentioned project, respective requirements for test and training must also be defined.

- For purposes of general coordination of all BCP activities in the Swiss financial market and to provide a platform to regularly discuss updates possibly necessary to cater for new developments, the steering committee chaired by the Swiss National Bank SNB will meet as needed, usually in yearly intervals.

The following options to provide the normative basis for the implementation of the agreed standards were analysed:

- Relying on instruments of public law (e.g. amendment of the ordinance of the Swiss National Bank SNB, circular from the Swiss Federal Banking Commission SFBC);
- Conclusion of contractual agreements by the parties involved;
- Self regulation (e.g. via the Swiss Bankers Association or via the central infrastructures);
- Optional implementation of the recommendations (especially when the number of institutions affected is limited).

The body responsible for providing the normative basis can either be the Swiss National Bank SNB or the Swiss Federal Banking Commission SFBC. In addition, such rules can either be directed directly at participants or indirectly via the rules of central infrastructures. Using the indirect route via the rules of central infrastructures offers the advantage that participants from abroad can also be made subject to them.

It has been decided that the normative basis shall be provided by relying on the existing ordinance issued by the Swiss National Bank covering its responsibilities to oversee

[5] In the meantime, the important participants have been defined. A threshold of a 5% or slightly below value share in the identified critical business processes was applied.

settlement systems for systemic risk purposes, applying both a direct and an indirect approach: The Swiss National Bank SNB agrees with system operators conditions that are subsequently implemented by these system operators for themselves and, where applicable, included in their rules that are binding for their system participants.

In addition, contacts with the communication sector will be intensified, as this sector plays a key role in all BCP preparations of the financial markets. This will be done within the Swiss national crisis precaution activities.

Appendix

Distribution of Transaction Values in SIC (first three quarters 2004)

Transaction Value (in CHF)	Number of Transactions (in %)[6]	cumulative	Total Value (in %)[7]	cumulative
<5'000	85.16	99.11	0.34	3.89
5'000 to <10'000	5.57		0.18	
10'000 to <50'000	5.43		0.56	
50'000 to <100'000	1.21		0.40	
100'000 to <500'000	1.45		1.47	
500'000 to <1 Mio	0.29		0.94	
1 Mio to <5 Mio	0.48	0.48	4.71	4.71
5 Mio to <10 Mio	0.09	0.09	2.95	2.95
10 Mio to <50 Mio	0.16	0.32	17.00	88.48
50 Mio to <100 Mio	0.06		19.65	
100 Mio to <200 Mio	0.09		41.57	
200 Mio to <300 Mio	<0.01		1.13	
300 Mio to <400 Mio	<0.01		0.68	
400 Mio to <500 Mio	<0.01		0.53	
500 Mio to <600 Mio	<0.01		0.44	
600 Mio to <700 Mio	<0.01		0.30	
700 Mio to <800 Mio	<0.01		0.23	
>800 Mio	<0.01		6.92	

The table clearly reveals that the trigger amount for large value payments for BCP purposes should be either CHF 10 Mio (88.48% of total value with 0.32% of number of transactions) or CHF 5 Mio (91.43% of total value with 0.41% of number of payments) or CHF 1 Mio (96.14% of total value with 0.99% of number of payments).

[6] The average number of payments per day in this period was 783'000 (with a maximum of 2,166 Mio payments on 27 February 2004).

[7] The average total value of payments per day in this period was CHF 166 billion (with a maximum of 217 billion on 30 April 2004).