Business Continuity Planning Finanzplatz Schweiz

Gemeinsames Papier einer Industriegruppe des Finanzplatzes Schweiz

Januar 2006

Business Continuity Planning Finanzplatz Schweiz – Inhaltsverzeichnis

1. Einführung und Management Summary

Die Akteure des Finanzplatzes Schweiz[1] beschlossen 2004, eine Bestandesaufnahme der allgemeinen Vorbereitung im Bereich Business Continuity Planning (BCP) auf dem Finanzplatz Schweiz durchzuführen. Es galt, Lücken und Verbesserungsmöglichkeiten festzustellen und Vorschläge zu unterbreiten. Dieses Dokument enthält eine Zusammenfassung der Ergebnisse.

Ziel der Analyse ist, die Stabilität des Finanzplatzes Schweiz bei grossen Störfällen sicherzustellen. Sie konzentriert sich auf die Stabilität des Finanzsystems und beschränkt sich folglich auf die grossen Marktteilnehmer des Finanzplatzes Schweiz. Aktivitäten ausschliesslich im Zusammenhang mit Retail-Finanzdienstleistungen werden nicht berücksichtigt.

Im Rahmen der Analyse wurden die folgenden Arbeitsschritte durchgeführt:

- Identifikation der systemkritischen Geschäftsbereiche der grossen Marktteilnehmer: Grossbetragszahlungsverkehr im Swiss Interbank Clearing SIC und Liquiditätsversorgung via Repos
- Definition der zu berücksichtigenden Störfälle (‚Ereignisszenarien'): physischer Ausfall eines beliebigen, wichtigen Gebäudes einschliesslich der darin befindlichen Mitarbeiterinnen und Mitarbeiter
- Gruppierung aller betroffener Institutionen: Marktinfrastrukturen einschliesslich der zentralen Buchungführungsinfrastruktur der Schweizerischen Nationalbank, des automatischen Repo-Handelssystems von Eurex/Swiss Exchange SWX, der Wertpapierabrechnungssysteme SECOM/SIS bei SegaInterSettle, der Zahlungsverkehrsysteme Swiss Interbank Clearing SIC/Telekurs einerseits und kritische Systemteilnehmer andererseits
- Beurteilung der aktuellen BCP-Vorkehrungen der identifizierten Institutionen
- Erarbeitung von BCP-Grundsätzen für den Finanzplatz Schweiz
- Aufbau einer interinstitutionellen Alarm- und Krisenorganisation für den gesamten Finanzplatz
- Identifikation weiterer Verbesserungsmöglichkeiten

Als allgemeines Ziel wurde die Anforderung festgelegt, dass die systemkritischen Marktinfrastrukturen bei grossen Störfällen innerhalb von zwei Stunden wiederhergestellt sein sollten und dass wichtige Teilnehmer dieser Infrastrukturen die Verarbeitung kritischer Geschäftstransaktionen innerhalb von vier Stunden wieder aufnehmen sollten. Dieses allgemeine Ziel entspricht auch den international auf anderen Märkten vorgesehenen Anforderungen.

Insgesamt kann der Vorbereitungsstand bei allen an der Arbeitsgruppe beteiligten Institutionen als gut bezeichnet werden. Es wurden Verbesserungsmöglichkeiten identifiziert, und die entsprechenden Massnahmen werden im Laufe der Zeit umgesetzt.

Vier BCP-Grundsätze wurden definiert und drei Projekte im Hinblick auf weitere Verbesserungen identifiziert. Als Sofortmassnahme wurde eine Alarm- und Krisenorganisation auf Interbankebene geschaffen.

[1] Schweizerische Nationalbank SNB, Eidgenössische Bankenkommission EBK, Credit Suisse, UBS, PostFinance, SIS Group, Swiss Exchange SWX und Telekurs Group

Die normative Basis für die Umsetzung der vereinbarten Normen bildet die bestehende Verordnung der Schweizerischen Nationalbank sowie die Anwendung eines direkten und indirekten Ansatzes: Die Schweizerische Nationalbank SNB vereinbart mit den Systembetreibern Auflagen, die diese dann für sich selbst umsetzen und, wo erforderlich, im Rahmen ihrer Regelwerke an ihre Systemteilnehmer weitergeben.

Des Weiteren sind die Kontakte zum Sektor Kommunikation auszubauen, da diesem für den Finanzmarkt bezüglich BCP eine Schlüsselrolle zukommt. Dies kann im Rahmen der nationalen Krisenvorsorge erfolgen.

2. Allgemeine BCP-Zielsetzungen

Der Finanzplatz besteht aus einem Netz von miteinander verbundenen Märkten, Marktinfrastrukturen und -teilnehmern. Die Funktionsweise jedes Teilnehmers an diesem Netz kann Auswirkungen über den eigenen Betrieb hinaus haben, andere Institutionen des Netzes betreffen und zu grossräumigen Störungen des Finanzplatzes insgesamt mit Folgen für die ganze Wirtschaft führen. Aufgrund der Wechselwirkungen innerhalb des Finanzmarktes und der Bedeutung für die Gesamtwirtschaft hat jede Institution eine Rolle zur Sicherung der Systemstabilität wahrzunehmen. Parallel dazu ist ein Gleichgewicht zwischen den Risiken und den Kosten für die Vorbereitungsmassnahmen zu schaffen.

Für die Zwecke dieses Berichts wird die folgende BCP-Begriffssystematik verwendet:

1. Präventivmassnahmen vor dem Eintritt eines Störfalls, um diesen zu verhindern, z.B. Bewachung, Firewalls etc.
2. Vorsorgemassnahmen vor dem Eintritt eines Störfalls, um einen eingetretenen Störfall zu bewältigen mit dem Ziel
    a. einer raschen Wiederherstellung der Standardprozesse (z.B. mit Back-up-Systemen)
    b. einer temporären Anwendung von Alternativprozessen, welche ohne die im Alltagsgeschäft eingesetzten IT-Anwendungen betrieben werden können, um während einer Übergangszeit die wichtigsten Geschäftstransaktionen zu bewältigen.

Die allgemeine Widerstandsfähigkeit des Finanzplatzes Schweiz bei einem Störfall muss die folgenden allgemeinen Zielsetzungen erfüllen:

- Verhindern, dass sich ein Störfall bei den als kritisch eingestuften Geschäftsbereichen auf den gesamten Finanzplatz auswirkt.

  Dieses Ziel wird durch die rasche Wiederaufnahme der Verarbeitung in der betroffenen Institution gestützt auf die ordentliche Betriebsinfrastruktur oder das Ausweichen auf Alternativprozesse als Übergangslösung erreicht.
- Erhalt eines hohen Vertrauens in die Wirksamkeit der BCP-Vorkehrungen.

  Regelmässige Verwendung der Alternativvorkehrungen und Back-up-Verfahren (Schulung und Tests), um sicherzustellen, dass diese Massnahmen umsetzbar sind und glaubwürdig bleiben.

- Gewährleistung einer Vorbereitung, die im Störfall ein koordiniertes Vorgehen erlaubt («prepare for the unexpected»).

  Eine solide Alarm- und Krisenorganisation auf interinstitutioneller Ebene, die jederzeit und schnell aufgeboten werden kann, gewährleistet einen Rahmen zur Koordinierung aller Tätigkeiten beim Auftauchen irgendwelcher Störfälle. Die Krisenorganisation muss regelmässig beübt werden.

Die Ausführungen dieses Dokuments beziehen sich auf die Stabilität des Finanzplatzes Schweiz. Deshalb wurden nur die betroffenen Geschäftsbereiche grosser Teilnehmer des Schweizer Finanzmarktes untersucht. Die Definitionen und Prioritäten wurden entsprechend festgelegt. Die übrigen Tätigkeiten wie Retail-Finanzdienstleistungen sind nicht Gegenstand des Berichts, obwohl sie für die Wirtschaft insgesamt und die Bevölkerung allgemein ebenfalls wichtig sein können.

3. Abgrenzungen

Business Continuity ist ein breites Thema. Abgrenzungen und Prioritätensetzungen sind daher unbedingt nötig. Um ein hohes Mass an Vertrauen zu gewährleisten, ist bei diesen Abgrenzungen, den Kriterien und Prioritäten volle Transparenz erforderlich.

Im Rahmen dieser Studie wurden die Abgrenzungen zu folgenden Punkten untersucht:

- Geschäftsprozesse
- Geschäftsfunktionen
- Ereignisszenarien
- Geschäftseinheiten

3.1 Geschäftsprozesse

Die folgenden Geschäftsprozesse wurden aus Sicht der Systemstabilität als zentral für den Finanzplatz Schweiz identifiziert:

- Grossbetragsüberweisungen über das Swiss Interbank Clearing SIC (Finanzzahlungsverkehr) und
- Liquiditätsversorgung über den Repo-Markt.

Diese beiden Geschäftsprozesse sind für das Funktionieren des Schweizer Finanzplatzes unerlässlich.

Eine allgemein akzeptierte Definition des Begriffs «Grossbetragszahlung» gibt es nicht[2], [3]. Die Festlegung, ob eine Zahlung als «Grossbetragszahlung» gilt, ist relativ und hängt auch von der Grösse des an der Zahlungstransaktion beteiligten Instituts ab (Auswirkung auf die

[2] Die Definition für «large value payments» im BIZ-Bericht «A glossary of terms used in payments and settlement systems» lautet «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» und führt noch nicht zu einer für BCP-Zwecke nutzbaren Abgrenzung.

[3] Bei der Einführung von SIC vor mehr als 15 Jahren wurde auf Zahlungen ab CHF 1 Million abgestellt, die ab dem Einführungstag zur Vermeidung von Liquiditätsstörungen zwingend via SIC abzuwickeln waren.

Liquidität). Eine Analyse der Zahlungsbeträge im SIC ist im Anhang zu diesem Bericht. Anhand dieser Zahlen drängt sich eine Betragsgrenze von CHF 1 Million oder CHF 5 Millionen auf.

Allerdings müssen auch Zahlungen in kleineren Beträgen, z.B. CLS Pay-In, als sehr dringend und wichtig erachtet werden. Aus diesem Grund muss ein Teilnehmer den Zahlungsverkehr bei einem Störfall gemäss einer Prioritätenordnung (Verarbeitung der dringendsten Zahlungen zuerst) gewährleisten. Der Wert einer einzelnen Zahlung ist nur ein Aspekt bei der Prioritätenfestlegung.

Aus Sicht der Systemstabilität wurden der Retail-Zahlungsverkehr (inkl. Debit- und Kreditkarten), die Bargeldversorgung (Banknoten) und der Wertpapierhandel lediglich als zweitrangig eingestuft. Mit den in diesem Bericht vorgeschlagenen Massnahmen wird jedoch die Situation bei den Retail-Zahlungen ebenfalls verbessert (z.B. Alarm- und Krisenorganisation, Verfügbarkeit des SIC, weil dieses auch die grossen Volumen an Retail-Zahlungen verarbeitet). Die Erfahrung in bisherigen Ausnahmesituationen zeigt, dass der Wertpapierhandel zu Recht als zweitrangig eingestuft wurde. Die Börsen wurden bis zur Beruhigung der Lage an den Finanzmärkten sogar bewusst geschlossen.

3.2 Geschäftsfunktionen

Es ist unerlässlich, dass für als zentral eingestufte Geschäftsprozesse die entsprechenden Geschäftsfunktionen verfügbar sind.

Bei der Untersuchung des Vorbereitungsstands der einzelnen Institute wurden die folgenden Geschäftsfunktionen besonders geprüft:

- IT
  - physische Infrastruktur wie Rechenzentren, Software etc.
  - personelle Ressourcen für den IT-Betrieb
- Business
  - physische Infrastruktur für die Geschäftstätigkeit wie Büros, Arbeitsplätze etc.
  - personelle Ressourcen für die Nutzung der Business-Anwendungen

3.3 Ereignisszenarien

Die Arbeitsgruppe analysierte und kategorisierte die folgenden möglichen Ereignisse:

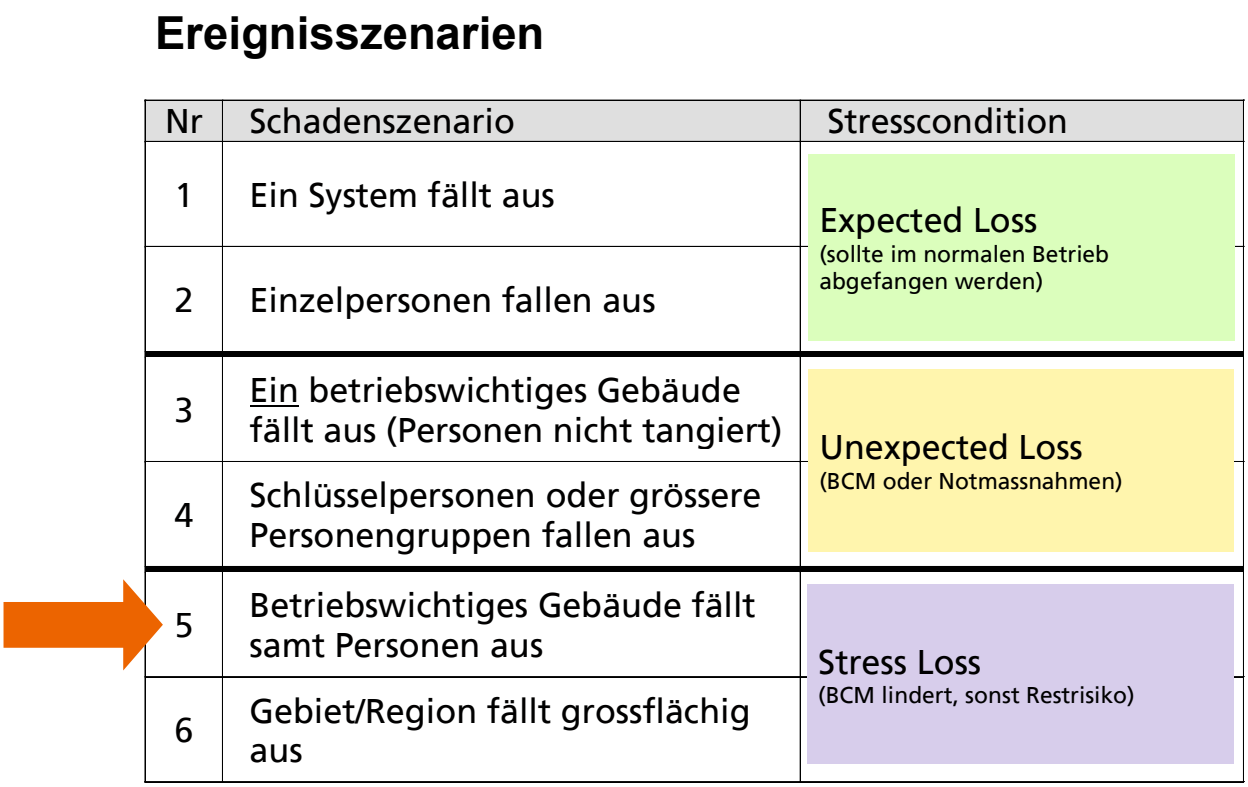

Abbildung 1: Ereignisszenarien

Es besteht ein breiter Konsens, dass sich die BCP-Analysen für den Finanzplatz Schweiz auf das Level 5 obiger Darstellung, den Ausfall eines betriebswichtigen Gebäudes inklusive des darin beschäftigten Personals, konzentrieren sollen. Level 1 bis 4 sind jeweils unternehmensintern abzudecken. Sie sind implizit in den Vorkehrungen für Level 5 enthalten.

Die Ursache für den Ausfall eines betriebswichtigen Gebäudes (technische Panne, Unfall, Anschlag, Naturereignis, Quarantäne zufolge einer Epidemie etc.) spielt keine Rolle. Mit der Konzentration auf Level 5 der oben dargestellten Ereignisszenarien wird gleichzeitig die Analyse von kumulativen Ereignissen an mehreren Standorten ausgeschlossen. Solide Vorbereitungen für Level 5 in allen betroffenen Institutionen tragen allerdings ebenfalls zur Bewältigung solcher Ereignisse bei.

Einen Sonderfall stellen in dieser Hinsicht Probleme bezüglich System- oder Anwendungssoftware und Datenverarbeitungssysteme dar. Sie sind in Level 1 enthalten und somit unternehmensintern abzudecken. Ein Problem in einem dieser Bereiche legt in der Regel sowohl den Hauptstandort als auch den Zweitstandort der betroffenen Institution lahm, da beide mit der gleichen Software und den gleichen Daten betrieben werden. Derartige Situationen können sich sowohl plötzlich wie auch über mehrere Tage ergeben. Im aktuellen Umfeld ist die Wahrscheinlichkeit eines derartigen Ereignisses höher einzuschätzen als das Auftreten rein physisch bedingter Störfälle, für die umfangreiche Vorbereitungen getroffen worden sind. Allerdings ist gleichzeitig festzuhalten, dass Vorsorgemassnahmen zur Bewältigung eines solchen Ereignisses, z.B. die Bereitstellung vollständiger Ausweichlösungen für System- und Anwendungssoftware extrem schwierig und nur mit sehr hohen Kosten umsetzbar sind. Präventive Massnahmen sind daher in diesem Bereich von erstrangiger Bedeutung.

3.4 Geschäftseinheiten

Zum Zweck dieser Analyse werden die betroffenen Institutionen wie folgt eingeteilt:

- **Zentrale Infrastrukturen** und
- angeschlossene Finanzinstitute (**kritische Systemteilnehmer**)

Für Institutionen dieser beiden Gruppen können unterschiedliche Anforderungen für die Bewältigung von Ausnahmesituationen gelten, insbesondere was die maximale Dauer eines Ausfalls betrifft. Dabei werden an die zentralen Infrastrukturen höhere Anforderungen gestellt als an die kritischen Systemteilnehmer. Für die kritischen Systemteilnehmer gelten wiederum höhere Anforderungen als für die übrigen Teilnehmer.

Als zentrale Infrastrukturen für die identifizierten besonders kritischen Geschäftsprozesse sind zu betrachten:

- Schweizerische Nationalbank SNB: Sie stellt die liquiden Mittel zur Verfügung und führt die Zahlungsabwicklungskonten
- Eurex/SWX: Repo-Handel
- SECOM/SIS: Repo-Abwicklung
- SIC/Telekurs: Zahlungsverkehr

Bei den kritischen Systemteilnehmern stellt sich die Frage nach der objektiven Definition. Im Allgemeinen wird dabei der Anteil an dem von der zentralen Infrastruktur verarbeiteten Wert oder Volumen verwendet. Mit Anteilen von 5-20% gilt ein Teilnehmer als kritisch. Eine Anwendung dieser Grenzwerte auf die Schweiz würde zu folgenden Zahlen der als kritisch zu erachtenden Systemteilnehmer führen:

Geschäftsprozess	Anzahl einzubeziehender Teilnehmer	
	20%	5%
Grossbetragsüberweisungsverkehr	1-2	3-4
Liquiditätsversorgung/Repo	1-2	5-6[4]

Es ist schwierig, für die Bestimmung der kritischen Systemteilnehmer der Schweiz einfach Marktanteilzahlen aus dem Ausland zu übernehmen. Eine analytisch saubere und zu begründende Abgrenzung ist im Grunde genommen nur durch vollumfängliche Simulationen möglich: Welche Teilnehmer sind für einen reibungslosen Betrieb der zentralen Infrastruktur unerlässlich?

Der am Volumen oder Wert gemessene Marktanteil jedes Teilnehmers kann allerdings auch irreführend sein. Einige Teilnehmer an zentralen Infrastrukturen nutzen gemeinsame Versorgungsdienste oder den selben Dienstleister für die Verbindung zur zentralen Infrastruktur. Solche Kombinationen können zu einer Situation führen, in denen die einzelnen Einrichtungen nicht als kritisch erachtet werden, zusammen aber den Grenzwert erreichen. Deshalb wurde beschlossen, solche Kombinationen bei der Festlegung der kritischen Systemteilnehmer zu berücksichtigen.

[4] 1 oder 2 davon mit Sitz ausserhalb der Schweiz

4. Bestehende Regeln und Vorsorgemassnahmen

Die Arbeitsgruppe befasste sich im Rahmen ihrer Analyse auch mit den bestehenden Regeln und Vorsorgemassnahmen auf internationaler und nationaler Ebene.

Auf internationaler Ebene lag der Hauptschwerpunkt beim Interagency White Paper der US-Aufsichtsbehörden.

Im Inland bieten das neue Nationalbankgesetz, mit dem der Schweizerischen Nationalbank SNB die Rolle der Systemüberwachung übertragen wird, und die von der SNB erlassene Verordnung mit Mindestanforderungen für systemkritische Abwicklungsinfrastrukturen eine BCP-Grundlage. Gemäss Verordnung müssen Betreiber systemkritischer Marktinfrastrukturen hohe Anforderungen hinsichtlich Zuverlässigkeit, Integrität, Vertraulichkeit und interner Kontrolle sowie anerkannte Sicherheitsnormen erfüllen. Die Praxis der SNB zur Umsetzung ihrer neuen Befugnisse ist noch nicht im Detail bekannt. Die kritischen Systembetreiber gemäss SNB-Verordnung sind festgelegt worden (SIC, SIS x-clear, SIS SegaInterSettle und CLS Bank). Das Mandat der SNB zur Systemüberwachung gemäss Nationalbankgesetz umfasst jedoch die Handelssysteme nicht.

Zudem bestehen Vorgaben der Eidgenössischen Bankenkommission EBK für die von ihr beaufsichtigten Institute (Banken und Effektenhändler). Diese Vorgaben befassen sich aber nicht explizit mit dem Thema «Business Continuity», sondern sind im Begriff der «ordnungsgemässen Geschäftsführung» eingeschlossen. Im Rahmen der Vorbereitungen auf das Jahr 2000 gab die EBK ein Rundschreiben heraus, in dem die Banken verpflichtet wurden, eine Notfallplanung auszuarbeiten. Die EBK geht davon aus, dass die ihr unterstellten Institute die Notfallplanung nicht nur auf ein einziges Ereignis bezogen, sondern auf allgemeinerer Basis erstellt haben und diese laufend aktualisieren und weiterentwickeln.

Die Schweiz verfügt auch über eine umfassende Organisation für alle Arten von extremen Vorfällen (Wirtschaftliche Landesversorgung WL). Die WL ist für die Versorgung des Landes mit lebenswichtigen Gütern und Infrastrukturen in Krisensituation zuständig. In diesem Zusammenhang ist für den Finanzsektor die Telekommunikation von ganz besonderer Bedeutung. Während andere Versorgungselemente der Infrastruktur wie Elektrizität, Wasser etc. durch eigene Vorkehrungen der einzelnen Institutionen zumindest kurzfristig aufgefangen werden können (z.B. durch Notstromaggregate), besteht eine unvermeidliche Abhängigkeit von einer funktionsfähigen Telekommunikation. Für die Abwicklung der identifizierten kritischen Geschäftsprozesse spielt die Telekommunikationsinfrastruktur generell eine entscheidende Rolle.

Die Kompetenzen in diesem Bereich werden durch zwei Artikel der Bundesverfassung geregelt (Art. 102 über die Landesversorgung und Art. 185 über die äussere und innere Sicherheit). Besonders wichtig ist in Krisenlagen Art. 185, der dem Bundesrat die Kompetenz zum direkten Erlass von Verordnungen und Verfügungen gibt. Basierend auf diesem Artikel können auch anderen zuständigen Stellen Befugnisse zur dringenden Bewältigung schwieriger Situationen eingeräumt werden. Diese Befugnisse dürften jedoch nur in sehr extremen Lagen zum Einsatz gelangen.

5. Ergebnisse und Empfehlungen

Die Arbeitsgruppe führte eine detaillierte Analyse der bestehenden Vorsorgemassnahmen bei den einzelnen Institutionen durch.

Ingesamt gelangte die Arbeitsgruppe zum Schluss, dass der Vorbereitungsstand der einzelnen Einrichtungen gut ist. Man war jedoch der Meinung, es lohne sich, die Vorbereitungen in einen noch zu schaffenden Gesamtrahmen von Grundsätzen einzubetten.

5.1 Grundlegende Anforderungen an die maximale Ausfallzeit

Die Grundvorgabe für zentrale Infrastrukturen und kritische Systemteilnehmer lässt sich wie folgt zusammenfassen:

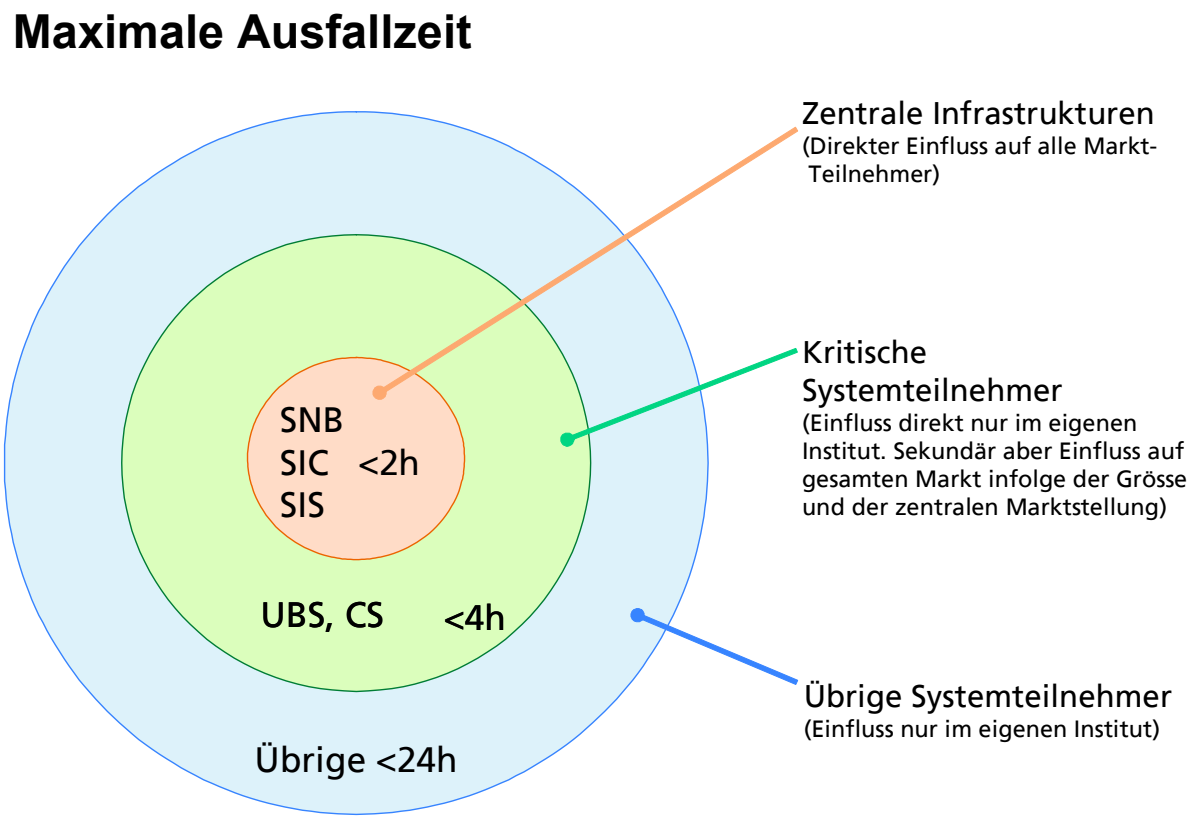

Abbildung 2: Maximale Ausfallzeit

Als Richtwert gilt, dass die identifizierten kritischen Geschäftsprozesse der zentralen Infrastrukturen bei einem Störfall in einem Schlüsselgebäude innert zweier Stunden wieder anlaufen müssen. Bei den kritischen Systemteilnehmern beträgt die maximale Ausfallzeit für die identifizierten kritischen Geschäftsprozesse vier Stunden. Für alle weiteren Systemteilnehmer gelten die Auflagen der Eidgenössischen Bankenkommission EBK, soweit sie der schweizerischen Bankengesetzgebung unterstellt sind. Die Vorsorgemassnahmen der zentralen Infrastrukturen und kritischen Systemteilnehmer sind so zu gestalten, dass diese Richtwerte unter normalen Umständen eingehalten werden können. Die Grundanforderungen lehnen sich eng an das US Interagency White Paper an.

5.2 Beurteilungen und Feststellungen

Die Analyse der Arbeitsgruppe führte zu folgenden Beurteilungen:

- Insgesamt können die Vorbereitungen der Marktinfrastrukturen und kritischen Systemteilnehmer als gut bezeichnet werden.

- Die räumliche Distanz zwischen Primär- und Sekundärstandort ist gemessen an internationalen Tendenzen häufig unterdurchschnittlich.
  In dieser Hinsicht sind allerdings drei Punkte zu berücksichtigen:
  - Distanz an sich kann nicht das alleinige Beurteilungskriterium sein. Die Schweizerische Nationalbank nimmt diesen Punkt in ihrer Verordnung auf und bestimmt, dass die zwei Standorte sich durch unterschiedliche Risikoprofile auszeichnen müssen.
  - Für den Rechenzentrumsbetrieb ist eine Interessenabwägung zwischen Distanz und Qualität vorzunehmen (Aktualität der Daten, Datenverlust, gute Reaktionsfähigkeit bei alltäglichen Störfällen).
  - Die technischen Möglichkeiten verbessern sich zwar laufend, aber die Investitionszyklen sind ebenfalls zu berücksichtigen. Die Einführung jeder neuen, technisch verfügbaren Möglichkeit würde zu riesigen laufenden Investitionen führen (‚alle zwei Jahre ein neues Rechenzentrum 20 Kilometer weiter weg'), die wirtschaftlich nicht tragbar wären.

  Die Anforderungen an die räumliche Distanz zwischen Primär- und Sekundärstandort müssen laufend aktualisiert und dabei die möglichen künftigen Gefahren beurteilt werden.

- Tests im IT-Bereich erfolgten bisher zur Vermeidung von Risiken im Alltagsbetrieb aufgrund des Datenrekonstruktionstests meistens auf vorbereiteter Basis. Es ist wichtig, dass laufend versucht wird, die Tests so realitätsgerecht wie möglich durchzuführen, ohne zusätzliche Risiken für den Normalbetrieb einzugehen.

- Die Vorsorgemassnahmen der einzelnen Institutionen sind im Allgemeinen eher auf den Ausfall physischer Komponenten (Hardware, Gebäude) als den Verlust von Personal ausgerichtet.

- Sobald Gebäude ‚multifunktional' genutzt werden (z.B. Rechenzentrum, IT- und Geschäftspersonal im selben Gebäude), entstehen durch die Kumulation zusätzliche Risiken bei einem extremen Störfall. Diese Risiken müssen berücksichtigt werden.

- Für die spezifische Situation und Marktstruktur der Schweiz gibt es bis heute keine Benchmark zur Bezeichnung der kritischen Systemteilnehmer.
  Durch den Einsatz von Alternativprozessen für die identifizierten kritischen Geschäftsprozesse und deren Nutzung durch alle wichtigen Systemteilnehmer sowie die Unterstützung mittelgrosser und kleinerer Systemteilnehmer in der Nutzung dieser Alternativprozesse durch die zentralen Infrastrukturen wird die Definition kritischer Systemteilnehmer weniger wichtig.

Ausserdem drängen sich die folgenden Feststellungen auf:

- Angesichts der konkreten Bedrohungslage stellt sich die Frage, ob die Vorbereitung auf Probleme mit System- oder Anwendungssoftware bzw. von Datenverarbeitungssystemen ausreichend berücksichtigt wird. Solche Störfälle müssen als wahrscheinlicher bezeichnet

werden als physische Störfälle, für die Vorkehrungen getroffen wurden.
Mit Ausnahme von SIC verlässt man sich diesbezüglich auf Präventionsmassnahmen, während Vorsorgemassnahmen selten sind. Bei MiniSIC stellt sich zudem die Frage, ob die Stapelverarbeitung (Batch Processing) überhaupt den heutigen Anforderungen noch gerecht werden kann (zum Beispiel zeitkritische CLS-Zahlungen bzw. Remote-Teilnehmer im SIC). Andererseits wäre ein Batch-Betrieb unter MiniSIC bei einem SIC-Störfall für die meisten heute über SIC abgewickelten Retail-Zahlungen ausreichend.

- In Ausnahmesituationen kann es sinnvoll sein, ‚Zeit zu kaufen', indem kurzfristig ein Geschäfts- zu einem Bankfeiertrag im SIC erklärt wird. Die Folgen eines solchen Schrittes sind zurzeit nicht bekannt – weder rechtlich noch betrieblich (z.B. im SIC-Vorvalutafile gespeicherte Zahlungen).

5.3 Schlussfolgerungen und Grundsätze

Die nachstehenden Schlussfolgerungen und Grundsätze wurden verabschiedet:

1. Bei den für die identifizierten kritischen Geschäftsprozesse nötigen zentralen Infrastrukturen bei der Schweizerischen Nationalbank SNB (für Repo-Handel und Kontoführung/Überwachung im Zusammenhang mit SIC), bei Telekurs (für SIC) und bei SIS SegaInterSettle (für SECOM/Repo) müssen sehr hohe Anforderungen an kurze Ausfallzeiten ohne Verlust von Daten über bestätigte Geschäftsvorfälle erfüllt werden. Die Ausfallzeit sollte grundsätzlich nicht mehr als zwei Stunden betragen. Dies gilt für alle Arten von Störfällen.

   Begründung: Für diese zentralen Infrastrukturen bestehen keine Alternativen (auch MiniSIC stellt in diesem Sinne keine Alternative für die identifizierten kritischen Geschäftsprozesse dar). Ein Ausfall dieser zentralen Infrastrukturen würde zu einem De-facto-Stillstand des Finanzplatzes Schweiz führen.

2. Für kritische Systemteilnehmer sollten ebenfalls hohe Anforderungen gelten. Sie sollen innerhalb von vier Stunden den Betrieb für die definierten kritischen Geschäftsprozesse wieder aufnehmen können.

   Wie die kritischen Systemteilnehmer dieser Anforderung gerecht werden, bleibt diesen im Einzelnen überlassen. Als Optionen stehen die Wiederaufnahme der Prozesse durch die normale Betriebsinfrastruktur innerhalb dieser Frist oder die Umstellung auf Alternativprozesse als Übergangslösung zur Verfügung.

   Auch bei der Nutzung der Option Alternativprozesse gelten hohe Anforderungen zur Wiederaufnahme des Normalbetriebs, da die Verwendung von Alternativprozessen nur eine Übergangslösung bieten kann. Die Verwendung von Alternativprozessen im Störfall erfordert auch umfassende Vorbereitungen (z.B. Verfügbarkeit von Kundenaufträgen und Geschäftstransaktionen).

   Begründung: Ohne die Verfügbarkeit von (kritischen) Systemteilnehmern ist die Vorsorge bei den wichtigen zentralen Infrastrukturen nur von beschränktem Nutzen. Der Einsatz von Alternativprozessen, die für eine Überbrückungszeit nach einem Störfall zum Tragen kommen und die Abwicklung einer begrenzten Zahl besonders wichtiger Geschäftsvorfälle sicherstellen, würde aus folgenden Gründen ein besonders

stabiles Sicherheitsnetz darstellen:

a. Die Alternativprozesse können allen wichtigen Systemteilnehmern verfügbar gemacht bzw. von ihnen bereitgestellt werden, nicht nur von denen, die als besonders kritisch erachtet werden. Verschiebungen in der Marktstruktur, die sehr kurzfristig erfolgen und dazu führen, dass weitere Systemteilnehmer als kritisch einzustufen sind, können auf diese Weise sofort und einfacher berücksichtigt werden.

b. Auf die Alternativprozesse kann bei Störfällen unabhängig von der Ursache rasch umgeschaltet werden. Die Umstellung kann sogar in weniger als vier Stunden erfolgen, weil die Umstellung auf den Alternativprozess sowie die Rückumstellung auf Normalbetrieb keiner grossen unmittelbaren Vorbereitung bedürfen (Beispiel: Nach dem Ausfall des Rechenzentrums kurz vor Abschluss der CLS-Bank-Verarbeitung können einige CLS-Zahlungen über den Alternativprozess laufen, während die Suche nach der Ursache im Rechenzentrum beginnt). Die Einfachheit der Umstellung in beide Richtungen erleichtert auch die Entscheidung zugunsten eines solchen Schrittes.

c. Die Alternativprozesse stehen unabhängig von der Ursache des Störfalls zur Verfügung. Sie decken insbesondere auch System- oder Anwendungssoftware- sowie Datenstörfälle (die das primäre und das sekundäre Rechenzentrum betreffen) ab.

Die Voraussetzungen für die systematische Nutzung von Alternativprozessen zu vertretbaren Kosten sind günstig. Einige Systemteilnehmer, darunter die beiden grössten, verfügen bereits über technische Installationen, um den Alternativprozess bei einem Störfall selbst zu betreiben. Für die übrigen (kritischen) Systemteilnehmer, deren jeweiliges Volumen bereits deutlich geringer ist, könnte die nötige Infrastruktur durch die zentralen Infrastrukturen in ihrem Namen («acting on behalf of») bereitgestellt werden.

3. Für den Repo-Handel auf SWX/Eurex können weniger weit gehende Anforderungen festgelegt werden, da bereits ein Alternativprozess definiert ist, der kurzfristig für die Abwicklung der wichtigsten Repo-Geschäfte zum Einsatz gelangen kann.

   Begründung: Dieser Alternativprozess bietet eine Möglichkeit zur Abdeckung weitergehender Störfallszenarien.

4. Der Prävention von system- oder anwendungssoftware- sowie datenbasierten Störfällen kommt insbesondere bei den zentralen Infrastrukturen von SNB, Telekurs/SIC und SIS/SECOM besondere Bedeutung zu. Die diesbezüglichen Präventionsmassnahmen sind laufend zu überprüfen und auf höchstem Stand zu halten.

   Begründung: Diese zentralen Infrastrukturen sind von erstrangiger Bedeutung, und es gibt nur begrenzte Alternativen für ihre Dienstleistungen.

   Zusätzlich sollte geprüft werden, wie innerhalb der alltäglichen funktionalen Trennung zwischen den Systemen von SNB und SIC eines der beiden Systeme Aufgaben des anderen übernehmen kann, um eine begrenzte Fortführung der Verarbeitung

sicherzustellen (z.B. Betrieb des SNB-Systems mit von den Teilnehmern via SWIFT angelieferten Grossbetragszahlungen bei Ausfall von SIC bzw. Vortrag der Tagesendsaldi auf den nächsten Tag innerhalb von SIC bei Ausfall der SNB).

5.4 Interbank-Alarm- und Krisenorganisation

Die Vorbereitungs- und Vorsorgemassnahmen können zwangsläufig nie alle Vorfälle so abdecken, wie sie in der Realität vorkommen. Es gibt immer Ereignisse, welche die bisherige Vorstellungskraft übersteigen. Deshalb müssen Strukturen geschaffen werden, die auch auf unerwartete Situationen reagieren können und flexibel bleiben, um sich an die Ereignisse anzupassen.

In einem solchen Fall müssen alle betroffenen Institutionen sehr schnell miteinander Kontakt aufnehmen und die notwendigen Massnahmen koordinieren können.

Aus diesem Grund hat die Arbeitsgruppe beschlossen, eine Alarm- und Krisenorganisation auf Interbankebene einzusetzen. Sie dient der Diskussion von Fragen, die über die im Rahmen dieses Berichts identifizierten kritischen Geschäftsprozesse hinausgehen, und dem Treffen der erforderlichen Entscheidungen:

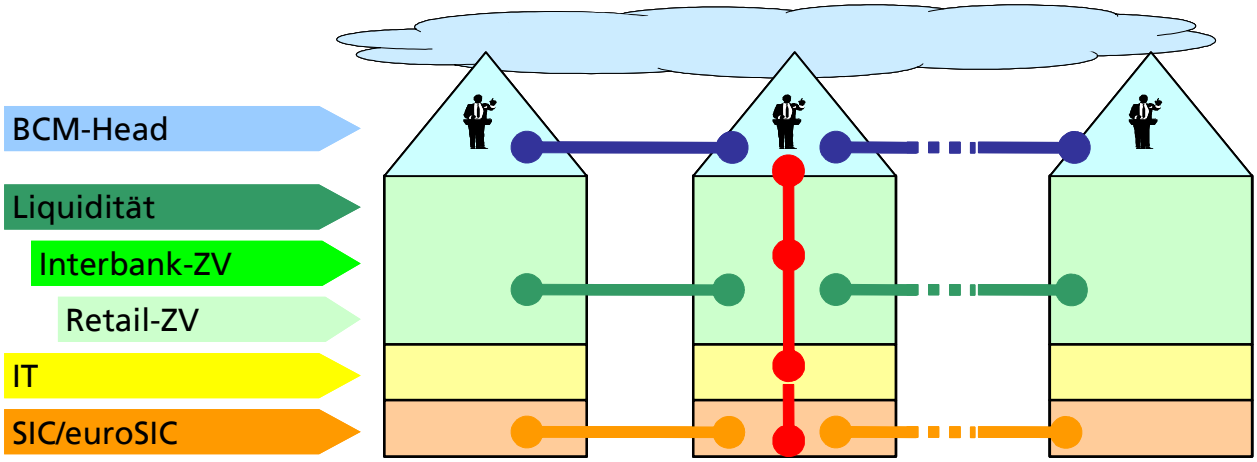

Abbildung 3: Interbank-Alarm- und Krisenorganisation

Die oberste Ebene der Interbank-Alarm- und Krisenorganisation bildet je ein Verantwortlicher oder eine Verantwortliche der BCP-Organisation der beteiligten Institutionen. Auf den unteren Ebenen (Liquidität, Zahlungsverkehr, SIC) werden auch Ansprechpartner in den einzelnen Unternehmen benannt. Sie bieten eine Kommunikationsplattform, wenn detaillierteres problem- und prozessspezifisches Wissen erforderlich ist. Bei einem Störfall kann jedes beteiligte Institut die Alarmorganisation auslösen. Dieses Institut hat auch die initiale Führung in der Krisenorganisation, bis eine andere Führung vereinbart wird. Für Krisenvorsorge und Krisenbearbeitung sowie die Bewältigung des eigenen Störfalls bleibt jedes Institut selbst verantwortlich. Sobald die Alarmorganisation aufgeboten und solange sie nicht aufgelöst worden ist, wird auch die Kommunikation nach aussen innerhalb dieser Krisenorganisation koordiniert. Die Alarm- und Krisenorganisation ist Gegenstand regelmässiger (jährlicher) Tests und Schulungen.

6. Nächste Schritte und Umsetzung

Jede Institution bleibt für die Umsetzung der im eigenen Unternehmen festgelegten Massnahmen verantwortlich. Auf Interbankebene wurden folgende Projekte berücksichtigt:

- Detaillierte Einigung über die Vorbereitungen für die vorgeschlagene BCP-Gesamtlösung einschliesslich Schaffung der Voraussetzungen für Alternativprozesse und ein «acting on behalf of» (Verantwortung: bestehende Interbank-Arbeitsgruppe PAP) sowie Definition kritischer Teilnehmer an den Marktinfrastrukturen (Verantwortung: Schweizerische Nationalbank SNB)[5]

- Beurteilung der Möglichkeit, einen «short notice bank holiday» im Swiss Interbank Clearing SIC zu erklären (Verantwortung: PAP; zur Diskussion der Rechtsfragen wird eine gemischte Arbeitsgruppe aus Rechtsexperten unter Führung eines Bankvertreters eingesetzt)

- Analyse der Möglichkeiten, im Rahmen der alltäglichen funktionalen Aufteilung zwischen den Systemen der Schweizerischen Nationalbank SNB und dem Swiss Interbank Clearing SIC dafür zu sorgen, dass bei Ausfall eines Systems das andere einige ausgefallene Funktionen übernehmen kann, damit eine begrenzte Fortführung der Verarbeitung gewährleistet ist (Verantwortung: SNB in Koordination mit PAP)

  In diesen drei Projekten sind jeweils auch die Anforderungen bezüglich Tests und Schulung zu definieren.

- Zur Gesamtkoordination aller Aktivitäten im Bereich BCP Schweiz sowie zur Bereitstellung einer Plattform für regelmässige Diskussionen über möglicherweise notwendige Aktualisierungen zur Berücksichtigung neuer Entwicklungen wird sich das Steuerungsgremium unter dem Vorsitz der Schweizerischen Nationalbank SNB bei Bedarf, in der Regel jährlich, treffen.

Die folgenden Optionen als normative Grundlage für die Umsetzung der vereinbarten Normen wurden analysiert:

- Nutzung öffentlich-rechtlicher Instrumente (z.B. Anpassung der SNB-Verordnung, EBK-Rundschreiben),
- Abschluss von privatrechtlichen Vereinbarungen zwischen den betroffenen Parteien,
- Selbstregulierung (z.B. über die SBVg oder Trägerschaft von zentralen Infrastrukturen),
- Freiwillige Umsetzung der Empfehlungen (insbesondere wenn die Zahl der betroffenen Institutionen begrenzt ist).

Das zuständige Gremium für die Bereitstellung der normativen Grundlage ist entweder die Schweizerische Nationalbank SNB oder die Eidgenössische Bankenkommission EBK. Ausserdem können solche Regeln direkt an die Systemteilnehmer gerichtet oder indirekt über die Systembetreiber erlassen werden. Der Vorteil der indirekten Umsetzung über die Regeln der zentralen Infrastrukturen liegt darin, dass ihnen auch Systemteilnehmer aus dem Ausland unterstellt werden können.

[5] Die kritischen Systemteilnehmer sind inzwischen definiert worden. Als Kriterium wurde eine Grenze von 5% (oder knapp darunter) des Wertanteils an den identifizierten kritischen Geschäftsprozessen angewandt.

Es wurde beschlossen, dass sich die normative Grundlage auf die bestehende Nationalbankverordnung, die ihre Verantwortung für die Beaufsichtigung des Zahlungsverkehrs hinsichtlich Systemrisiken abdeckt, und auf einen indirekten Weg abstützen soll: Die Schweizerische Nationalbank SNB vereinbart mit den Systembetreibern Auflagen, die diese dann für sich selbst umsetzen und, wo erforderlich, in die Regeln aufnehmen, die für ihre Systemteilnehmer verbindlich sind.

Des Weiteren werden die Kontakte zum Sektor Kommunikation ausgebaut, da diesem für den Finanzmarkt bezüglich BCP eine Schlüsselrolle zukommt. Dies erfolgt im Rahmen der nationalen Krisenvorsorge.

Anhang

Betragsverteilung im SIC (erste drei Quartale 2004)

Transaktionswert (in CHF)	**Anzahl Transaktionen (in %)**[6]	**kumuliert**	**Wert total (in %)**[7]	**kumuliert**
<5'000	85,16	99,11	0,34	3,89
5'000 bis <10'000	5,57		0,18	
10'000 bis <50'000	5,43		0,56	
50'000 bis <100'000	1,21		0,40	
100'000 bis <500'000	1,45		1,47	
500'000 bis <1 Mio.	0,29		0,94	
1 Mio. bis <5 Mio.	0,48	0,48	4,71	4,71
5 Mio. bis <10 Mio.	0,09	0,09	2,95	2,95
10 Mio. bis <50 Mio.	0,16	0,32	17,00	88,48
50 Mio. bis <100 Mio.	0,06		19,65	
100 Mio. bis <200 Mio.	0,09		41,57	
200 Mio. bis <300 Mio.	<0,01		1,13	
300 Mio. bis <400 Mio.	<0,01		0,68	
400 Mio. bis <500 Mio.	<0,01		0,53	
500 Mio. bis <600 Mio.	<0,01		0,44	
600 Mio. bis <700 Mio.	<0,01		0,30	
700 Mio. bis <800 Mio.	<0,01		0,23	
>800 Mio.	<0,01		6,92	

Die Tabelle zeigt deutlich auf, dass die Betragsgrenze für BCP-Zwecke entweder bei CHF 10 Millionen (88,48% des Umsatzes mit 0,32% der Zahlungen) oder bei CHF 5 Millionen (91,43% des Umsatzes mit 0,41% der Zahlungen) oder bei CHF 1 Million (96,14% des Umsatzes mit 0,99% der Zahlungen) anzusetzen ist.

[6] Die durchschnittliche Anzahl Zahlungen pro Tag betrug im angegebenen Zeitraum 783 000 (mit einem Maximum von 2166 Millionen Zahlungen am 27. Februar 2004).

[7] Der durchschnittliche Umsatz pro Tag betrug im angegebenen Zeitraum CHF 166 Milliarden (mit einem Maximum von 217 Milliarden. am 30. April 2004).