EZB-Definitionen wichtiger BC-Begriffe im Zusammenhang mit Zahlungs- und Wertpapierabwicklungssystemen[1], Juni 2007

Nachstehende Definitionen wurden auf ESZB-Ebene vereinbart und basieren auf folgenden Quellen:

1. Business continuity oversight expectations for systemically important payment systems (SIPS), EZB, Juni 2006
2. Glossary of terms ECB (erarbeitet und verwendet für das BCM der EZB)
3. Glossary of General BC Management Terms, The Business Continuity Institute (BCI) Dezember 2002
4. BC Glossary, Disaster Recovery Journal und Disaster Recovery Institute International (DRJ)
5. NZBen der EU
6. High-level principles for business continuity, Joint Forum, Basler Ausschuss für Bankenaufsicht, August 2006

Allgemeine Begriffe	Definition
Notfallverfahren (Business Contingency)	Unter Contingency-Verfahren (Notfallverfahren) werden technische und organisatorischeBackup-Verfahren verstanden, die Teil des Business-Continuity-Plans sind, und darauf abstellen, Dienstleistungen während der Ausfallzeit in begrenztem Umfang - z. B. im Zahlungsverkehr für besonders kritische Zahlungen wie CLS-Zahlungen – zur Verfügung zu stellen (normalerweise mit Hilfe von Alternativ- oder Ersatzverfahren).
Geschäftsfortführung im Krisenfall (Business Continuity)	Zustand eines unterbrechungsfreien Geschäftsbetriebs. Unter „Business Continuity“ werden alle organisatorischen, technischen und personellen Maßnahmen, verstanden, die zur Fortführung(i)der Kerngeschäfte unmittelbar nach Eintritt des Krisenfalls und (ii) sukzessive des gesamten Geschäftsbetriebes bei länger andauernden und schweren Störungen dienen.
Management der Geschäftsfortführung im Krisenfall (Business Continuity Management (BCM))	Ganzheitlicher Managementprozess, der potenzielle Risiken einer Organisation identifiziert und einen Rahmen für den Aufbau seiner Widerstandsfähigkeit bietet, um die Organisation in die Lage zu versetzen, wirksam zu reagieren und die Interessen ihrer wichtigsten Akteure sowie ihre Reputation, Markenzeichen und wertschöpfenden Aktivitäten abzusichern.
Plan zur Geschäftsfortführung im Krisenfall (Business-Continuity-Plan)	Ein klar definierter und dokumentierter Maßnahmenplan, um eine kontinuierliche Geschäftstätigkeit bei Eintreten eines Not-, Ereignis- oder Katastrophenfalles und/oder einer Krise zu ermöglichen. Ein Business-Continuity-Plan wird auch als Disaster Recovery Plan (DRP - Plan zur Wiederherstellung des Betriebs im Katastrophenfall) bezeichnet.
Strategie hinsichtlich der Geschäftsfortführung im Krisenfall (Business-Continuity–Strategie)	Ansatz, der es einer Organisation ermöglicht, die Wiederherstellung und Aufrechterhaltung einer kontinuierlichen Geschäftstätigkeit im Katastrophenfall oder angesichts eines anderen größeren Ausfalls sicherzustellen. Die Pläne und Verfahren dazu richten sich nach der jeweiligen Strategie der Organisation. Es kann mehrere Lösungsansätze geben, um die Strategie einer Organisation zu erfüllen. Beispiele: Interner oder externer „heißer“ Rechenzentrum (Hot Site) oder „kalter“ Rechenzentrum (Cold Site), Gegenseitigkeitsabkommen über Ausweicharbeitsplätze, Mobile Recovery, rasche und zuverlässige Lieferung (Quick Ship) / Direktversand (Drop Ship), konsortiumsweite Lösungen, usw.

[1] HAFTUNGSAUSSCHLUSS: Die Begriffe wurden anlässlich des auf ESZB-Ebene stattfindenden Austauschs von Informationen zur Business Continuity festgelegt.

Team für die Durchführung von Massnahmen, die der Geschäftsfortführung im Krisenfall dienen (Business Continuity Management Team)	Kreis von Personen mit bestimmten Funktionen und Zuständigkeiten bei der Umsetzung des Business-Continuity-Plans.
Krisenmanagement (Crisis management)	Prozess, mit dem eine Organisation die weiteren Auswirkungen von Business-Continuity-Notfällen/-Ereignissen/-Krisen bewältigt, bis diese entweder unter Kontrolle oder ohne Folgewirkung für die Organisation eingedämmt sind oder auf den BCP als Teil des Krisenmanagementprozesses zurückgegriffen wird.
Testen	
(Simulations-) Übung ((Simulation) Exercise)	Durchführung eines Business–Continuity-Plans für ein bestimmtes simuliertes Szenario, um die Wirksamkeit und denVorbereitungsstand zu testen und/oder die Notwendigkeit zur Entwicklung zusätzlicher Pläne aufzuzeigen. Die Übung dient dem Zweck der Schulung und desTrainings der Mitglieder des Teams und der Verbesserung ihrer Leistungsfähigkeit sowie der Überprüfung des Business–Continuity-Plans. Die Übungen beinhalten u. a.: Tabletop-Übungen (Theoretische Diskussionen), Simulationstests, Funktionsfähigkeitstests, simulierte Katastrophen, Schreibtisch-Übungen und Vollübungen (Tests aller Abläufe).
Test	Tätigkeit, bei der ein Teil oder mehrere Teile eines Business-Continuity-Plans abgearbeitet werden, um sicherzustellen, dass der Plan die richtigen Informationen enthält und das gewünschte Resultat erzielt wird. Ein Test unterscheidet sich von einer Übung, als dass er am realen Standort durchgeführt wird, während eine Übung in der Regel als Simulation erfolgt.
Walkthrough	Durchdenken eines Problems (Walkthrough), bei dem versucht wird das wahrscheinliche Ergebnis / die wahrscheinlichen Ergebnisse eines Ereignisses basierend auf Anfangsbedingungen, Begleitumständen und Auswirkungen von Entscheidungen herauszufinden. Im Kontext der Geschäftsfortführung im Krisenfall (Business Continuity) soll mit einem Walkthrough i) sichergestellt werden, dass Pläne zur Geschäftsfortführung im Krisenfall für diesen Fall geeignet sind ii) der Informations- und Entscheidungsprozess eines Krisenteams bewertet und iii) mögliche Lücken identifiziert werden.
Wiederherstellung und Wiederanlauf	
Wiederherstellung (Recovery)	Wiederherstellung bestimmter Geschäftstätigkeiten nach einer Störung auf ein Maß, das ausreicht, um ausstehende Verpflichtungen zu erfüllen.
Spätester Zeitpunkt der Wiederherstellung (Recovery Point Objective)	Zeitpunkt, zu dem die Wiederaufnahme der Geschäftstätigkeit nach einem Ereignis-/ Stör-/Krisenfall, durch den die Fortführung des Geschäftsbetriebs unterbrochen/gestört wurde, wieder möglich sein sollte, z. B. „Geschäftstagesbeginn“.
Zeitspanne für die Dauer der Wiederherstellung (Recovery Time Objective - RTO)	Zeitspanne, innerhalb derer Systeme, Anwendungen oder Funktionen nach einem Ausfall wiederhergestellt sein sollten (z. B. ein Geschäftstag). RTOs dienen häufig als Basis zur Entwicklung von Recovery-Strategien und zur Klärung der Frage, ob die Recovery-Strategien im Katastrophenfall anzuwenden sind oder nicht.
Wiederanlauf (Resumption)	Prozess der Planung und/oder Durchführung des Neustarts von bestimmten Geschäftsfunktionen und –tätigkeiten nach einer Katastrophe.
Standorte	
Datenzentren mit Lastverteilung (Load sharing data centers)	Zwei (oder mehrere) Datenzentren, die IT-Aufgaben jeweils zu gleichen Teilen abarbeiten. Beide Datenzentren sind im Normalzustand produktiv, und die Arbeit wird gleichmäßig unter ihnen aufgeteilt. Sie verfügen beide über ausreichend Kapazität, um bei Ausfall des einen Datenzentrums die Arbeitsbelastung des anderen vollständig übernehmen zu können.

Zweites Rechnersystem (Secondary site)	Ausweichrechner, der sich an einem anderem Standort als der Produktionsrechner befindet und von Systemen und/oder Personen genutzt werden kann, um den Geschäftsbetrieb und sonstige Funktionen im Not- und Katastrophenfall, bei Auftreten größerer Störungen im System und Fehlfunktionen der Infrastruktur oder bei fehlender Zugriffsmöglichkeit auf den Hauptrechner wieder aufzunehmen. Das Zweite Rechnersystem kann wie folgt genutzt werden: - im engeren Sinne: für die Replizierung von Programmen und Daten zur Sicherung der Datenintegrität. Die replizierten Daten werden extern gespeichert und gewährleisten die Wiederaufnahme des Geschäftsbetriebs im Falle der Zerstörung oder des Verlusts von Daten. - im weiteren Sinne: für das Vorhalten eines umfassenden Ausweichsystems (Hardware, Software, Daten) im Falle der Nichtverfügbarkeit des Produktionssystems (Fallback-System). Sofern sich das Fallback-System in der Nähe des Produktionssystems befindet und für den Not- und Katastrophenfall (NuK-Fall) ein drittes System an einem anderen Standort vorgehalten wird, wird dieses als NuK-System (Disaster System) bezeichnet. Das Zweite Rechenzentrum kann „kalt" oder „heiß" sein. **Kaltes Rechenzentrum (Cold site)** – ein Ausweich-Rechenzentrum mit Grundausstattung, das bereits über die notwendige Infrastruktur verfügt, um kritische Geschäftsfunktionen oder Informationssysteme wiederherzustellen, in dem aber keine Computer-Hardware, Telekommunikationsgeräte, Kommunikationskanäle usw. vorinstalliert sind. Diese müssen zum Zeitpunkt des Eintretens der Katastrophe installiert werden. **Heißes Rechenzentrum (Hot site) –** ein Ausweich-Rechenzentrum, das bereits über die notwendige Ausstattung wie Rechner, Telekommunikationsgeräte und umgebender Infrastruktur verfügt, damit kritische Geschäftsfunktionen im Katastrophenfall mit minimaler Verzögerung fortgeführt werden können. Ähnliche Begriffe: **Ersatzrechner, Ausfallrechner, Backup-Rechner, Datenzentren mit Lastverteilung (Load sharing data centers).**
Ereignisse	
Krise (Crisis)	Eintreten und/oder Wahrnehmung einer Bedrohung für Geschäftsbetrieb, Mitarbeiter, Shareholder Value, Akteure, Markenzeichen, Reputation, Vertrauen und/oder strategische Ziele/Geschäftsziele einer Organisation.
Katastrophe (Disaster)	Jegliche außerplanmäßige Unterbrechung einer oder mehrerer aufgabenrelevanter Geschäftsfunktionen über einen inakzeptabel langen Zeitraum hinaus. Es wird unterschieden zwischen großflächiger/schwerer (large-scale/major), lokaler oder regionaler Katastrophe. **Großflächige/schwere Katastrophe (large-scale/major disaster)** – Ereignisfall (oder NuK-Fall), der ein großes Ballungs- oder geographisches Gebiet betrifft und eine weitreichende Störung des normalen Geschäftsbetriebs der Finanzmarktteilnehmer sowie sonstiger kommerzieller Einrichtungen verursacht und dazu führen kann, dass Zonen in einem bestimmten Umkreis vom Ort des Auftretens evakuiert werden müssen oder unzugänglich sind. **Lokale Katastrophe (local disaster)** – Ereignis (oder NuK-Fall), dessen unmittelbare negative Auswirkungen auf ein geographisches Gebiet im Umkreis von maximal wenigen Kilometern vom Ort des Auftretens begrenzt ist. **Regionale Katastrophe (regional disaster) –** Anders als eine lokale Katastrophe betrifft eine regionale Katastrophe eine ganze Region, die demselben Risikoprofil unterliegt.
Störung (Disruption)	Ereignis, das die Kontinuität/Funktionen des Systems unterbricht und es so an der Erfüllung seiner Aufgaben behindert. **Größere Betriebsstörung (Large-scale/Major operational disruption - MOD) –** Eine *größere Betriebsstörung* ist eine folgenschwere Störung des normalen Geschäftsbetriebs, die ein großes Ballungs- oder geographisches Gebiet und die darin wirtschaftlich integrierten anliegenden Gemeinden erfasst. Neben der Behinderung des Normalbetriebs der Finanzmarktteil-

	nehmer und anderer kommerzieller Organisationen wirken sich größere Betriebsstörungen typischerweise auf die physische Infrastruktur aus. Eine *größere Betriebsstörung* ist ein Ereignis, bei dem der Rückgriff auf die Business-Continuity-Pläne von mehr als einer Organisation erforderlich ist.
Notfall **(Emergency)**	Tatsächliche oder drohende Situation, die Schäden verursacht, Leben und Eigentum zerstört oder die Beeinträchtigung, den Verlust oder eine Störung des normalen Geschäftsbetriebs einer Organisation zur Folge haben kann und somit eine ernsthafte Bedrohung darstellt.
Rückgriff **(Fallback)**	Rückgriff auf Ausweichsysteme, wenn die Geschäftsprozesse wegen Nichtverfügbarkeit der Support-Systeme nicht im Normalbetrieb ausgeführt werden können.
Ausfall **(Outage)**	Zeitraum nach einer Störung, in dem Leistungen, Systeme, Prozesse oder Geschäftsfunktionen voraussichtlich unbrauchbar oder unzugänglich sind.
Kritische Funktionen	
Analyse der geschäftlichen Auswirkungen **(Business-Impact-Analyse (BIA))**	Strukturiertes Verfahren zur Messung der finanziellen und operationalen Auswirkungen einer Störung im Zeitverlauf.
Kerngeschäft **(Core business activities)**	Als Kerngeschäft werden diejenigen Geschäftsprozesse bezeichnet, die für das Erreichen der Unternehmensziele von vitaler Bedeutung sind und deren kurz- oder langfristiger Ausfall den Bestand des Unternehmens bzw. (bei Behörden) die Erfüllung hoheitlicher Aufgaben und die Stabilität des Finanzsystems existentiell gefährden würde.
Kritische Funktionen **(Critical functions)**	Geschäftstätigkeiten oder Informationen, deren mehrtägige Unterbrechung oder Nichtverfügbarkeit der Organisation erheblichen wirtschaftlichen Schaden zufügen, ihre Reputation schädigen oder ihren Betrieb ernsthaft gefährden würde.
„Einzige Quelle für einen Ausfall“ **(Single Point of Failure)**	Alleinige (einzige) Quelle einer Dienstleistung, Tätigkeit und/oder eines Prozesses, deren Ausfall zu einem vollständigen Ausfall einer kritischen Tätigkeit und/oder einer abhängigen Tätigkeit führen würde.
Kritische Einheiten	
Kritische (Infrastruktur-)Teilnehmer (Größere, bedeutende, zentrale, systemrelevante Teilnehmer/große Akteure) **(Critical (infrastructure) participant** (Major, relevant, core, systemically important participant/major player**))**	System- oder infrastrukturseitig identifizierte Akteure, bei denen der Ausfall ihres Normalbetriebs die ernsthafte Gefahr größerer Störungen für das System oder die Finanzinfrastruktur mit sich bringen würde.
Kritische (Markt-)Infrastrukturen **(Critical (market) infrastructure)**	Dazu zählen folgende Infrastrukturen: - Zahlungssysteme, die für die Stabilität des Finanzsystems von Bedeutung sind, - Wertpapierabwicklungssysteme, - zentrale Kontrahenten, - sonstige kritische Infrastrukturen im Zusammenhang mit Zahlungs- und Abwicklungssystemen gemäß nationalen Definitionen.
Kritische Anbieter von Dienst- und Versorgungsleistungen **(Critical providers of services and utilities)**	Anbieter von Dienstleistungen, Produkten und Lösungen gelten als kritisch, wenn die Nichterfüllung ihrer normalen Geschäftstätigkeit die ernsthafte Gefahr größerer Störungen für Systeme oder Infrastrukturen mit sich bringen würde.