EUROPEAN CENTRAL BANK

EUROSYSTEM

June 2007

ESCB definitions of major business continuity terms in relation to payment and securities settlement systems[1]

The ESCB has developed a glossary of major business continuity terms for market infrastructures, providing consistent and commonly agreed definitions for some of the most frequently used terms in national and EU-wide standards.

The aim of having such a glossary is twofold: (i) to allow the ESCB to use consistent definitions of terms in its own business continuity planning and procedures; and (ii) to enable market infrastructures and other interested parties, especially those with a cross-border presence, to take account of the generally accepted terms used by the central banking community in their own business continuity plans and procedures.

Unless otherwise indicated on their individual websites, all 27 national central banks of the ESCB apply the definitions contained in this glossary.[2] However, this is not the case for other central banks or entities other than central banks.

The definitions below have been agreed at the level of the ESCB and are based on the following sources:

1) Business continuity oversight expectations for systemically important payment systems (SIPS), ECB, June 2006;
2) ECB glossary of terms (developed and used for the ECB's business continuity management);
3) Glossary of General Business Continuity Management Terms, Business Continuity Institute (BCI), December 2002;
4) Business Continuity Glossary, Disaster Recovery Journal (DRJ) and Disaster Recovery Institute International (DRII); and
5) High-level principles for business continuity, Joint Forum, Basel Committee on Banking Supervision, August 2006.

[1] DISCLAIMER: These terms have been developed in relation to ESCB business continuity information-sharing for market infrastructures.

[2] National definitions posted on the business continuity sections of the websites of individual nationalentral banksgreed ESCB definitions.uch cases, the individual national central banks should explain the rationale for such differences on their own websites.

	Definition
General terms	
business contingency	Technical and organisational backup procedures, as part of a business continuity process, aimed at providing limited services (e.g. for particularly critical payment transactions such as CLS payments) during the outage period (usually by means of alternative or additional measures or procedures).
business continuity	A state of uninterrupted business operations. This term also refers to all of the organisational, technical and staffing measures employed in order to: (i) ensure the continuation of core business activities in the immediate aftermath of a crisis; and (ii) gradually ensure the continued operation of all business activities in the event of sustained and severe disruption.
business continuity management (BCM)	A holistic management process that identifies potential risks to an organisation and provides a framework for establishing resilience in order to ensure that the organisation is able to respond effectively in the event of a crisis and safeguard its reputation, brand and value-creating activities and the interests of key stakeholders.
business continuity management team	A group of people with defined roles and responsibilities as regards the implementation of the business continuity plan.
business continuity plan	A clearly defined and documented plan for use in the event of a business continuity emergency, disaster or crisis. Also referred to as a "disaster recovery plan" (DRP).
business continuity strategy	A strategy adopted by an organisation in order to ensure its recovery and continuity in the event of a disaster or other major outage. Plans and methodologies are determined by this strategy. There may be more than one means of carrying out an organisation's strategy (e.g. an internal or external hot or cold site, an alternative work area, a reciprocal agreement, mobile recovery, quick/drop shipping or consortium-based solutions).
crisis management	The process by which an organisation manages the wider impact of a business continuity emergency, disaster or crisis by seeking to control or contain the situation without affecting the organisation or, where this proves not to be possible, implementing its business continuity plan.
Testing	
simulation exercise	The execution of a business continuity plan in a specific simulated scenario with the intention of testing the effectiveness of the plan and the preparedness of the organisation and/or highlighting areas where the plan requires further development. This activity is performed with the aim of training team members, improving their performance and evaluating the business continuity plan.Types of exercise include: tabletop exercises, simulation exercises, operational exercises, mock disasters, desktop exercises and full rehearsals.
test	The carrying out of one or more parts of a business continuity plan in order to ensure that the plan contains the appropriate information and produces the desired result. A test differs from an exercise in that a test occurs at a real site, whereas an exercise is generally a simulation.
walkthrough	A walkthrough is a thought experiment that seeks to discover the likely outcome(s) of an event on the basis of starting conditions, surrounding conditions and the effects of decisions. In the context of business continuity, a walkthrough seeks: (i) to ensure that business continuity plans are fit for purpose; (ii) to assess a team's

	Definition
	information exchange and decision-making; and (iii) to identify any gaps.
Recovery and resumption	
recovery	The restarting of specific business operations following a disruption, with such operations reaching a level sufficient to meet outstanding business obligations.
recovery point objective	The point in time to which work should be restored (e.g. the start of the day) following a business continuity emergency, disaster or crisis that interrupts or disrupts business operations.
recovery time objective (RTO)	The period of time within which systems, applications or functions should be restarted following an outage (e.g. one business day). RTOs are often used as a basis for the development of recovery strategies and a means of determining whether or not to implement specific recovery strategies in a disaster situation.
resumption	The process of planning for and/or implementing the restarting of defined business functions and operations following a disaster.
Sites	
load-sharing data centres	Two (or more) data centres running IT tasks on an equal basis. Both are productive in normal situations and they carry out the same amount of work. Both data centres are designed with sufficient capacity margins to be able to take on the complete workload of the other data centre should it fail.
secondary site	A location other than the primary site which can be used for the resumption of business operations and other functions in the event of a disaster, a major system or infrastructure malfunction or an inability to access the primary site. A secondary site can be used: – in the narrower sense for the replication of programs and data in order to safeguard data integrity, with the replicated data being stored externally to ensure the resumption of business operations following the destruction or loss of data; or – in the broader sense for the maintenance of a comprehensive alternative system (i.e. a fallback system comprising hardware, software and data) to cater for the possibility of the production system not being available. In the event that the fallback system is located in the vicinity of the production system and a third system in another location is reserved for emergencies and disasters, the latter is referred to as the “disaster system”. A secondary site can be “cold” or “hot”. **Cold site:** An alternative facility that already has in place the basic infrastructure required to recover critical business functions or information systems, but does not have any preinstalled computer hardware, telecommunications equipment, communication lines, etc. These must therefore be installed at the time of the disaster. **Hot site:** An alternative facility that is already equipped with the computer, telecommunications and environmental infrastructure required to allow critical business functions to continue with minimal delay in the event of a disaster. Also referred to as an “alternative site”, a “backup site” or a “load-sharing data centre”.

	Definition
Events	
crisis	An event that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organisation.
disaster	Any unplanned interruption to one or more mission-critical business functions for an unacceptable period of time. A disaster can be large-scale/major, regional or local. **Large-scale/major disaster:** An event affecting a large metropolitan or geographical area that causes wide-scale disruption to the normal business operations of financial industry participants and other commercial entities. This may lead to areas within a given radius of the location of the event being evacuated or becoming inaccessible. **Regional disaster:** A disaster affecting a whole region with the same risk profile. **Local disaster:** A disaster the direct adverse effects of which are limited to a geographical area with a maximum radius of a few kilometres.
disruption	A breakdown in the continuity or functions of a system or organisation which prevents it from completing its tasks. **Large-scale/major operational disruption (MOD):** High-impact disruption to normal business operations affecting a large metropolitan or geographical area and the adjacent communities economically linked with it. In addition to impeding the normal operations of financial industry participants and other commercial organisations, major operational disruptions typically affect physical infrastructure. This kind of incident requires the implementation of the business continuity plans of more than one organisation.
emergency	An actual or impending situation that may cause injury, the loss of life or the destruction of property or may interfere with or disrupt an organisation's normal business operations to such an extent that it poses a threat.
fallback	Workaround procedures to be used in the event that normal business procedures cannot be conducted because supporting systems are not available.
outage	Period of time after disruption that a service, system, process or business function is expected to be unusable or inaccessible.
Critical functions	
business impact analysis (BIA)	A structured procedure measuring the financial and operational consequences of disruption over time.
core business activities	Business processes on which an organisation depends for the achievement of its goals. The unavailability of such processes, even in the short term, would seriously threaten the existence of the organisation or (in the case of public authorities) fundamentally jeopardise the execution of sovereign functions and endanger the stability of the financial system.
critical functions	Business activities or information that could not be interrupted or remain unavailable for several business days without incurring significant financial losses, damaging the reputation of the organisation or significantly jeopardising its operations.
single point of failure	A situation in which a service, activity or process is provided by one single source, the failure of which would lead to the total failure of a critical function.

	Definition
Critical entities	
critical (infrastructure) participant	An entity identified by the system or infrastructure as posing a threat in that there would be a significant risk of major disruption to the system or financial infrastructure were that entity unable to perform its normal operations. Also known as a "major participant", "relevant participant", "core participant", "systemically important participant" or "major player".
critical (market) infrastructure	Any of the entities listed below: – systemically important payment systems; – securities settlement systems; – central counterparties; and – other critical infrastructure related to payment and settlement systems in accordance with national definitions.
critical provider of services and utilities	A provider of services, goods and solutions that is critical in that there would be a significant risk of major disruption to systems or infrastructure were that provider unable to perform its normal activities.