Guidelines on business continuity for market infrastructures

1. Introduction

In July 2013 the Banca d'Italia issued a set of requirements for business continuity for banks (Annex A). The increasing complexity of financial business, the intensive use of information and communications technology, the interdependence among the various financial players, and the new risk scenarios require the establishment of a single framework for business continuity for market infrastructures and banks. Accordingly, the Banca d'Italia has adopted these requirements as standards for the performance of the functions in relation to market infrastructures assigned to it by the Consolidated Law on Banking (Legislative Decree 385/1993) and the Consolidated Law on Finance (Legislative Decree 58/1998).

These updated guidelines replace their predecessor documents[1], reflecting intervening changes in technology and the regulatory framework[2]. They are without prejudice to the application of the European and national regulations on business continuity and incorporate the standards adopted by the main international forums[3].

2. Scope of application

The annexed standards for business continuity are addressed to the operators of technological infrastructures or networks and to the operating companies of wholesale markets in government securities, multilateral wholesale trading facilities in government securities, multilateral deposit trading systems, securities settlement systems, central counterparties and central securities depositories with registered offices and/or operational headquarters in Italy (hereafter 'operators').

3. Proportionality principle

These standards take account of the size and operational complexity of the operators specified in the previous paragraph, the nature of their activity, and the type of service provided.

4. Market infrastructures providing essential services

Section III of the annexed standards concerns market infrastructures that provide essential services for payment systems and access to the financial markets; these infrastructures shall be identified in a communication from the Banca d'Italia. The communication shall specify the systemically important processes pertaining to each infrastructure. The list of the interested operators will be published on the website of Banca d'Italia.

---

[1] "Guidelines on business continuity in wholesale markets and support systems," October 2004; "Guidelines for the business continuity of payment system significant infrastructures", November 2004; "Guidelines for business continuity in central securities depositories, securities settlement systems and central counterparties", annex to measure of Banca d'Italia and CONSOB, 22 February 2008.

[2] EU Regulation 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories; Article 146 of the Consolidated Law on Banking as amended by Article 35(18) of Legislative Decree 11/2010; Articles 69, 69-bis, 76, 77, 77-bis, 79 and 82 of the Consolidated Law on Finance on the oversight of wholesale markets in government securities, on multilateral trading in monetary deposits in euros, on settlement systems for transactions in financial instruments, on trade repositories and central counterparties; and measure of Banca d'Italia and CONSOB, 22 February 2008 "Rules governing central depositories, settlement services, guarantee systems and related management companies".

[3] "Business continuity oversight expectations for systemically important payment systems", issued by Eurosystem in June 2006; "Principles for Financial Market Infrastructures" issued by Bank for International Settlements Committee on Payment and Settlement Systems (CPSS) and IOSCO Technical Committee, April 2012.

5. Risk assessment

For an overall risk assessment, the person responsible for business continuity planning at each institution should take part in the assessment of operational risk.

6. Self-assessment

As a helpful tool for business continuity management, the operators specified in paragraph 2 above shall carry out a self-assessment of their situation vis-à-vis the annexed standards (gap analysis) and shall specify a timetable and a set of procedures for adapting (an implementation plan).

ANNEX A

BUSINESS CONTINUITY REQUIREMENTS

SECTION I

GENERAL PROVISIONS

1. Introduction

The increasing complexity of financial business, the intensive use of information and communications technology, and the new risk scenarios require operators to step up their effort to guarantee adequate levels of business continuity.

To this end they shall adopt an extensive approach which, beginning with the identification of critical corporate processes, specifies for each of them organizational safeguards and business continuity measures commensurate with the level of risk.

The specific measures to adopt shall take account of international standards and best practices and/or of those laid down by trade associations.

2. Definitions

— "CODISE" ("Continuità di servizio", business continuity): coordinating body for operational crises in the Italian financial marketplace, chaired by the Banca d'Italia;
— "crisis": a situation of formally declared interruption or deterioration of one or more critical or systemically important processes as a consequence of incident or disaster;
— "escalation": management of an incident characterized by the involvement of progressively higher levels in the corporate hierarchy, where necessary reaching the board of directors;
— "emergency": a situation stemming from an incident or disaster in which the affected operator must take exceptional technical and operational measures for the prompt recovery of normal operation;
— "business continuity management": the set of initiatives aimed at reducing to what is deemed an acceptable level the damage resulting from incidents or disasters affecting an operator directly or indirectly;
— "business continuity plan": a formal document stating the principles, setting the objectives, describing the procedures and identifying the resources for business continuity management concerning critical and systemically important corporate process. The plan is generally divided into sectoral plans;
— "disaster recovery plan": a document establishing the technical and organizational measures to cope with events that put electronic data processing (EDP) centers out of service. The plan, which must permit important EDP procedures to be performed at standby facilities, is an integral part of the business continuity plan;
— "recovery point": the instant up to which the integrity of saved data is guaranteed at primary and standby facilities;
— "standby facility": an infrastructure that enables the operator to continue to carry out critical and systemically important processes, even in the event of incident or disaster that disables the primary facility;
— "primary facility": the infrastructure at which the operator's activities are normally conducted;

— “recovery time” of a process: the interval between the operator’s declaration of the state of crisis and the recovery of the process to a predetermined level of service. It consists of the time it takes:
  - to analyze the events and decide on the actions to take, before intervening;
  - to start again the process by means of technical and organizational interventions and the subsequent verification of the possibility of making the services available again without damage and in conditions of safety and security (“restart time”).

SECTION II

REQUIREMENTS FOR ALL OPERATORS

1. Scope of the business continuity plan

Operators shall establish a business continuity plan for coping with situations of crisis consequent to sectoral or company-level incidents or broader disasters striking the operator or significant counterparties (other group members, major suppliers, prime customers, specific financial markets, clearing, settlement and guarantee systems).

Business continuity plans shall envisage solutions not only based on technical and organizational measures to safeguard electronic databases and the operation of information systems but that also envisage contingencies of widespread crisis and prolonged blockage of essential infrastructures, so as to guarantee continuity of operation in the case of disasters.

Where some critical processes are carried out by specialized parties belonging to the group (e.g. the assignment of the ICT or back-office function to an instrumental company), safeguards for their business continuity must form an integral part of the operator's overall business continuity plan.

The business continuity plan must be part of the operator's overall risk management plan. It must take account of vulnerabilities and preventive measures taken to ensure the attainment of corporate objectives.

The business continuity plan must envisage several crisis scenarios based on at least the risk factors listed below, following from natural events or human activities, including serious damage caused by employees:

— destruction or inaccessibility of structures housing critical operational units or equipment;
— unavailability of critical information systems;
— unavailability of staff essential to corporate processes;
— interruption of operation of infrastructure (e.g. electricity, telecommunications, interbank networks, financial markets);
— alteration or loss of critical data and documents.

The business continuity plan shall specify the procedures for getting over the emergency, with special attention to damage assessment, the management of all the recovery operations, and checking the operational status of the services recovered.

2. Impact analysis

An impact analysis, preliminary to the drafting of the business continuity plan and regularly updated, should determine the level of risk for each corporate process and highlight the repercussions of a service outage. The residual risks, not handled by the business continuity plan, must be documented and explicitly accepted by the competent corporate bodies. Resource allocation and the priorities for intervention shall be commensurate with the level of risk.

The impact analysis shall take account of the parameters characterizing the corporate organization and operations, including:

— the specificities – in terms of probability of disaster – in connection with the location of important facilities (e.g., danger of earthquake, danger of floods and landslides, proximity to dangerous industrial sites, airports or institutions of symbolic significance);
— geographical concentration (e.g., presence of a large number of institutions in the centers of major cities);
— the degree of complexity of the institution's typical or prevalent activity and the degree of automation achieved;
— the size of the institution and the territorial distribution of activities;
— the extent of outsourcing of important functions (e.g. information systems and back-office);
— the relative centralization or decentralization of critical processes;
— constraints stemming from interdependence, as with suppliers, customers and other operators.

The impact analysis shall consider, in addition to operational risks, also such other risks as market and liquidity risk.

3. Drafting of the business continuity plan and crisis management

3.1 The role of corporate bodies

Business continuity must be adequately considered at all levels of responsibility. To this end, the board of directors shall:

a) establish the objectives and strategies for business continuity;
b) assign human, technological and financial resources sufficient to attain the objectives;
c) approve the business continuity plan and successive modifications resulting from technological and organizational adjustments, accepting the residual risks not covered by the business continuity plan;
d) be informed at least once a year of the results of checks on the adequacy of the plan and of the business continuity measures;
e) designate the person responsible for business continuity planning;
f) promote the development and regular checking of the business continuity plan and its adaptation to any significant organizational, technological or infrastructural innovations and in the case of detection of shortcomings or the materialization of new risks;
g) approve the annual plan for testing the business continuity measures in place and examine a written report on the results of the tests.

The body charged with the control function is responsible for verifying the completeness, adequacy, functionality and reliability of the business continuity plan.

Activities and decisions shall be properly documented.

3.2 Critical processes

Operators shall specifically identify most relevant processes relating to corporate functions whose non-availability - owing to the high impact of the resulting damage - necessitates high levels of business continuity to be achieved through preventive measures and business continuity solutions activated in case of incident.

To this end, special attention must be given to the processes relating to relations with customers, including firms and general government, and to the recording of transactions in the accounts.

For each critical process, the operator shall identify the person responsible, the IT support procedures, the staff assigned, the logistical structures involved, and the ICT infrastructures used.

The person responsible for the process shall determine, in observance of the strategic guidelines and rules laid down in the business continuity plan, the process recovery time and shall collaborate actively in designing business continuity measures.

3.3 Person responsible for business continuity planning

The person responsible for business continuity planning shall have an appropriate hierarchical rank and function. The person responsible for business continuity planning shall develop the business continuity plan, ensure its continuous updating in relation to significant organizational and technological changes, and verify its adequacy at least once a year. The person in this position shall also be the contact person for the Banca d'Italia in case of crisis.

Where the business continuity plan is divided into sectorial plans, the operator shall designate a referent for each of the latter. The sectoral referents shall coordinate, in the matters within their competence, the work to design and maintain the plans, implement the measures envisaged, and conduct testing[4]. Before activating new systems or processes, they shall prepare appropriate modifications to the plans.

3.4 The content of the business continuity plan

The business continuity plan shall specify the conditions and procedures for declaring the state of crisis, the organization and the procedures to follow in crisis situations, and the path for the return to normal operations.

The business continuity plan shall assign the power to declare a state of crisis and establish the chain of command for managing the operator in exceptional circumstances. There shall be measures for rapid escalation that make it possible, once the extent of the incident has been determined, to proceed rapidly to the declaration of a state of crisis.

The processes for the management of incidents and for the declaration and management of the crisis shall be formal and closely integrated with one another. To this end, the operator shall expressly identify the members of the structure for crisis management (e.g., a crisis committee), the person responsible for that structure, the chain of command, the internal communications procedures and the responsibilities attributed to the corporate functions involved.

The business continuity plan shall establish the recovery time for critical processes.

The business continuity plan shall identify standby facilities, provide suitable sites and logistical and communications infrastructures for the personnel involved in the crisis, establish the rules for retaining back-up copies of important documents (e.g. contracts) in remote locations from those where the originals are kept.

With reference to central and peripheral information systems, the business continuity plan shall include a disaster recovery plan[5]. The disaster recovery plan shall indicate the mode and

[4] Where the business continuity plan is not divided into sectorial plans, these activities shall be performed by the person responsible for business continuity planning.
[5] In the case of outsourcing of critical components of the information system, Section 3.7 shall apply.

frequency of generation of back-up copies of production files and the procedures for recovery at standby facilities.

The frequency of back-up shall be commensurate with the size and functions of the institution[6]. Production files of critical processes have to be backed up at least once a day. There shall be precautions for the prompt shipment and conservation of the electronic back-up copies in high-physical-security facilities located at a distance from the production systems[7].

The business continuity plan shall specify the modalities of communication with customers, significant counterparties, authorities and the media.

Standby facilities must be utilizable, in case of need, even for prolonged periods of time.

3.5 Testing

The procedures for testing business continuity measures depend on how critical the processes are and what risks are detected. As a consequence, the frequency and level of detail of the tests can vary. In some cases a partial simulation of the disastrous event may be sufficient; for critical processes, the test shall involve final users, service suppliers and, where possible, important counterparties.

At least once a year comprehensive tests shall be conducted, using scenarios as realistic as possible, of the operational recovery of critical processes in crisis conditions, checking the ability of the organization to implement the measures set out in the business continuity plan as scheduled.

In particular, the annual testing of information systems shall include the activation of network links with the standby facility and the execution of batch procedures testing the functions and the performance of the standby facilities. The tests should preferably be run on real production data.

The results of the tests shall be reported in writing, notified to the competent corporate bodies and transmitted, for the matters under their respective competence, to the operational units involved and to the audit function. Where the tests reveal shortcomings, appropriate corrective measures shall be taken promptly.

3.6 Human resources

The business continuity plan shall identify the staff essential to guarantee the continuity of critical processes and shall instruct this personnel in detail on the actions to take in case of crisis.

The business continuity procedures must be clear and detailed, so that they can be executed even by staff members not assigned to the ordinary activities to which the procedures refer.

The staff assigned to the business continuity plan shall be trained on the continuity measures, shall have access to the list of contacts and to the documentation necessary to operate in

[6] For example, if it serves as intermediary for indirect participants in settlement systems.

[7] For non-critical processes, there must in any case be procedures for acquiring and regularly managing back-up copies of data and software so as to ensure the integrity and availability of the data. For off-line standby facilities, in which data archives are not present or are not aligned with production data in real time, the modalities and timing of such alignment after recovery shall be specified.

crisis situations, shall be familiar with the standby facilities and the equipment, and shall take part in the tests of business continuity measures.

The operator shall consider the advisability of distributing the activities involving critical processes among more than one facility or organizing the staff's work in shifts.

3.7 Outsourcing, infrastructures and relevant counterparties

Where corporate functions connected with critical processes are outsourced, the business continuity plan shall specify the measures to take in case of crisis with significant impact on the institution or on the service provider.

The outsourcing contract shall formally state the service levels to be guaranteed in the case of crisis and the continuity provisions to be put in place by the service provider, in keeping with attainment of corporate objectives and with the indications of the Banca d'Italia. The contract shall also specify the mode of participation, direct or via user committees, in the testing of the service provider's business continuity plan.

The operator must acquire the service provider's business continuity plan or else must have adequate information to assess the quality of the measures envisaged and to integrate them with its own, internal continuity measures. The service provider shall notify the operator promptly of any incident in order to allow prompt activation of the business continuity procedures.

The operator's business continuity plan shall take into consideration the contingency of a disaster striking the main technological and financial infrastructures and/or important counterparties and shall specify the measures for coping with the resulting problems. The ability to communicate with the standby facilities of these counterparties must be verified regularly.

For the operator's essential services, consideration must be given to provision for recourse, in emergency, to alternative providers.

Where the service provider has engaged the same human resources in providing analogous services to other operators, especially if the latter are located in the same area, there shall be contractual safeguards to avoid the risk that in case of concomitant necessities of other organizations the quality of the service may deteriorate or the service become, de facto, unavailable.

3.8 Controls

The business continuity plan and its updating shall be checked regularly by the internal audit function, which shall examine the test programmes, take part in the tests and check the results, and suggest changes to the business continuity plan on the basis of the shortcomings found.

Special attention shall be paid to analysis of the criteria for escalation. In the case of incidents, the audit function shall evaluate the length of time required to declare the state of crisis. The function shall also be involved in testing the business continuity plans of outsourcers and other critical suppliers; it may decide to rely on the controls performed by the structures of the latter if they are deemed professionally capable, independent and transparent. The internal audit function shall examine outsourcing contracts to make sure that the level of safeguards is up to the corporate objectives and standards.

Operators shall consider the advisability of submitting their business continuity plans to competent, independent third parties for review.

3.9 Communications to the Banca d'Italia

In the case of crisis, after critical processes have been recovered, the operator shall communicate to the Banca d'Italia its assessment of the impact on the operations of its central and peripheral structures and on relations with customers and counterparties.

SECTION III

SPECIAL REQUIREMENTS FOR SYSTEMICALLY IMPORTANT PROCESSES

1. Introduction

The operation of the financial system as a whole depends on proper functioning of the largest operators and their ability to provide essential services in the payment system and for access to financial markets.

The Banca d'Italia can require these operators to comply with stricter business continuity requirements than those applying to all operators, in particular as regards the recovery time of systemically important processes (see Section 2.1), the location of standby facilities, and the resources allocated to crisis management.

The Banca d'Italia shall identify, by name, the operators to which special requirements apply, require adaptations of their business continuity plans, and check the solutions adopted. These operators shall take part in the CODISE's initiatives for coordination of financial system business continuity.

2. Design of the business continuity plan and crisis management

2.1 Systemically important processes

Processes that are critical to the Italian financial system, those that by contagion can cause a blockage of the entire domestic marketplace, are concentrated in the payment systems and the procedures for access to the financial markets.

For the purposes of the present provisions, these processes are defined as "systemically important processes" for business continuity of Italian financial system. The Banca d'Italia notifies each operator of the systemically important processes pertaining to it. They represent a structured set of activities directed to the provision of the following services:

- services in connection with the real-time gross settlement systems in central bank money (Target2), the central securities depositories, the central counterparties, and the securities settlement systems (Express II). They also comprise daily matching services for pre settlement of securities transactions;
- services in connection with access to markets relevant for the financial system's liquidity. They comprise: multilateral systems for the exchange of money deposits in euro (e-MID), ECB open market operations, Italian Treasury's auctions, and the wholesale REPO market on government securities (the REPO segment of MTS);
- retail payment services widely used by the general public. They comprise: postal money orders, payment of social pensions, cash provisioning;
- services strictly functional to the basic liquidity needs of economic agents, blockage of which has major negative impact on their operations. They comprise: the management of ICT infrastructures for cash dispensing via ATMs, support for applications and services under the SITRAD (Italian interbank data transmission network) convention.

2.2 Responsibilities

Operators shall:

— implement adjustments to their business continuity plans relevant to systemically important processes;

— ensure continuous compliance with the special requirements;

— designate a single person responsible for these activities.

2.3 Risk scenarios

The risk scenarios relevant to the continuity of systemically important processes shall be documented and regularly updated. In addition to what is prescribed for all operators, these scenarios shall include: disasters with large-scale material destruction on at least a metropolitan scale that affect the essential infrastructures of the operator and of third parties; severe crisis situations, even without material destruction (e.g., pandemics, biological weapons attacks, large-scale cyber-attacks).

2.4 Standby facilities

The standby facilities for systemically important processes shall be located at a suitable distance from their respective primary facilities so as to guarantee a high degree of independence between the two facilities.

In general, standby facilities shall be located outside the metropolitan area in which the primary facility is located; and they must be served by utilities (telecommunications, electricity, water, etc.) different from those serving the primary production facility. Where this is not the case, there must be a rigorous assessment, supported by the opinions of qualified third parties (e.g., the Civil Protection Department, academics, and professionals) and fully documented, that the risk of simultaneous unavailability at both primary and standby facilities is negligible.

Information system standby facilities shall be configured with a capacity sufficient, if needed, to handle the peak volumes recorded in the course of ordinary operations.

2.5 Recovery time and service availability

The recovery time for systemically important processes shall not exceed four hours. The restart time must not exceed two hours.

If a disaster at an operator causes the blockage of systemically important processes at other operators, the latter shall recover their own systemic processes within two hours from the renewed operation at the operator first affected by the disaster.

Where the risk scenarios (Section 2.3) result in especially severe impact, the recovery objectives can be adapted; this adaptation shall be notified to the operators affected by the Banca d'Italia, taking account of the indications agreed on with CODISE.

With regard to information systems, technological architectures providing for online duplication of operational data in such a way as to eliminate or minimize data loss shall be deemed adequate. To this end the time between the recovery point and the incident must be virtually zero.

Even in the case of extreme situations, there must be provisions for immediate or nearly immediate recovery of systemically important processes, including by means of procedures not completely integrated into corporate processes, as long as they are protected from the security standpoint (e.g. using offline PCs, faxes, and telephone contacts with selected counterparties), in particular in handling essential liquidity needs.

2.6 Resources

The business continuity plan shall specify the resources – human, technological and logistical – necessary to keep systemically important processes operating. It must ensure – by means of organizational measures, agreements with third parties, duplication of staff, or other documented measures – the presence at standby facilities, where needed, of the personnel required for the operation of the systemically important processes. Concentration of all the key personnel at a single place or time must be avoided.

2.7 Tests

At least once a year, the safeguards for continuity of the systemically important processes shall be carefully tested. Operators shall guarantee their active participation in tests and market-wide simulations organized or promoted by authorities, by markets and by the main financial infrastructures.

3. Communications to the Banca d'Italia

In the case of incidents that may have significant impact on systemically important processes, the declaration of the state of crisis shall be followed by the immediate request to activate CODISE, with an initial assessment of potentially damaged operators.

In the case of crisis, after critical processes have been recovered, the operator shall promptly communicate to the Banca d'Italia its assessment of the impact on the operations of its central and peripheral structures and on relations with customers and counterparties.

Systemically important operators shall transmit to the Banca d'Italia a yearly report on the main features of their business continuity plans, on the adaptations and additions implemented in the course of the year, on the checks conducted by the internal audit function, on the main incidents that occurred and on the recurrent criticalities.