GUIDELINES FOR BUSINESS CONTINUITY IN WHOLESALE MARKETS AND SUPPORT SYSTEMS

MARKET SUPERVISION OFFICE

October 2004

1. Introduction

Guaranteeing the efficiency and correct operation of money and financial markets and their support systems requires that trading and post-trading services be managed with special attention to the risks of information and telecommunications failure or inadequate functioning. The practical application of this principle is often restricted to the technological component. System operators have demonstrated sensitivity to the adverse circumstances that have been historically most likely to occur. Each operator has a “contingency plan” in case of disaster. The plans are designed to guarantee the continuity of vital operations and the restoration of acceptable operations within a predetermined deadline.

In recent years, however, decisive new factors have emerged, creating a more complicated and risky scenario, as well as a less predictable one. The traditional contingency tools are accordingly less appropriate and satisfactory. In particular, the events of September 11 in New York underscored the increased probability of major disasters. Together with the ever-increasing importance of the financial industry in the advanced countries, this warrants adequate, specific protection for the financial markets. The picture is further complicated by recent “disasters” linked to public utility failures.

This necessitates more highly articulated measures, more robust and effective solutions involving all agents who play important roles in the financial market product chain. The oversight authorities in the leading countries have undertaken a review of the relevant organizations' emergency preparedness. In this context in 2002 the Bank of Italy, in accord with Consob, undertook a series of initiatives with the participation of the components of the Italian financial marketplace (intermediaries, exchanges, support structures and payment systems). The plan is to study the current situation, see where improvements can be made, devise rules and instruments to improve system security and redesign an integrated set of procedures for emergency management.

The study phase confirmed the crucial importance of the service infrastructures for security markets, given their central role in the activities of intermediaries. The functions of clearing and settlement of financial instruments are of special importance. If problems in these services put “transaction execution” services out of operation, this could affect the continuity of markets and intermediaries. What follows is a set of guidelines that the companies that operate trading and post-trading services must follow to ensure business and operational continuity for their infrastructures. The guidelines apply to systems for wholesale trading in government securities and interbank deposits and for the clearing, settlement, guarantee and central deposit of financial instruments, as well as strictly connected and instrumental activities.

2. Objectives

The authorities' action seeks to strengthen the Italian financial system's capacity to withstand unforeseeable events. The ultimate objective is to limit the overall risk of such events. The intermediate objectives are to institute appropriate instruments for coping with crises and restoring normal operations of financial markets and their support systems. Depending of the dimensions of the disruptive event and the importance of the service affected, reactivation must be such as to return “rapidly” to “acceptable” system operations and close the business day. The restoration of “normal” operations must come within an “appropriately short” time.

These objectives require the reorganization of contingency plans to set concrete reference parameters for business continuity. General guidelines for limiting "systemic risk" are set out below. They are commensurate with the importance of the role played by the organizations to which they are addressed. The guidelines also set out the criteria for designing organizational and operational measures to improve and maintain emergency plans.

This initiative, together with similar actions vis-à-vis intermediaries and payment infrastructures undertaken on a cooperative basis by the Bank of Italy, completes the set of actions needed to reinforce the structures operating in the credit, money and financial sectors in Italy. Similar guidelines have been adopted by other countries with financial systems of comparable size. The principles reconcile conflicting exigencies due to the complexity of the problems and the need for stability of rules. Chiefly, therefore, they outline the strategies to follow and leave actual realization up to the system operators.

3. Business continuity and the operating companies

Business continuity is central to strategy of system operators. It requires assessment of the state of the system, appropriate management choices and the involvement of decision-making and control bodies. It is the duty of top management to set objectives on business continuity, select policies to attain them and design the consequent development and operations plans.

The business continuity plan should be approved by the Board of Directors. Its purpose is to cope with critical problems due to sectoral incidents or to broader disasters directly affecting the system or major counterparties (other closely linked systems, important suppliers, system members, essential financial infrastructures, and utilities).

As minimum requisites, the company's business continuity plan must:

- classify internal activities by their importance to the function performed;
- identify, for each activity, the objectives and technical and organizational measures needed;
- allocate sufficient resources to implement the plan;
- specify the frequency and scope of checks;
- name all those who must be involved in tests, including suppliers;
- examine the problems of outside service providers and the remedies adopted;
- design a system for assessing the plan and designing corrective measures;
- highlight possible interrelations with outside institutions, considering also cross-border activities.

The plan must consider at least the possible crisis scenarios set out below, with an impact analysis and description of possible solutions for each:

- non-availability of a building housing critical offices or services;
- sudden lack of essential staff;
- sudden absence of outside services (e.g. electricity, telecommunications networks, interbank networks, outsourced services, services essential to the financial system);
- attacks from outside or inside (e.g. computer viruses, attacks via telecommunications nets, damage from disloyal employees);
- major disasters.

The company's top management must institute organizational arrangements to define, maintain, monitor and manage business continuity (e.g., crisis and emergency operations committees),

assigning responsibilities for the management of the different phases of the emergency and assigning tasks in case of crisis vis-à-vis third parties and the authorities. To enhance the overall dependability of the plan, recourse to leading auditing firms with experience in international safety and security standards, or else certification procedures, is recommended. Top management should take part in the main choices involving business continuity. It should work for widespread familiarity with the plan among staff, for formal documentation and regular reporting to the Board of Directors and the Board of Auditors. The plan must be notified to the oversight authorities, which must be promptly informed of any changes or additions.

4. Requirements for the business continuity plan

4.1 Risk analysis

The priorities set and the resources allocated to business continuity have to be commensurate with the risks. A regularly updated analysis of the risks inherent in a set of scenarios examines the impact on every internal process and on vital and critical services to produce a gauge of the overall level of risk.

This analysis:

- *must be set in the internal context of the operator (e.g. its degree of organizational and operational complexity, its degree of automation) and in the external context (e.g., location of sites, nearness to likely targets, geographical concentration);*
- *must consider the functions that are outsourced (e.g. information systems, hardware facilities) and the elements involved in continuity of the outside suppliers;*
- *must thoroughly evaluate the constraints of interdependence with and among suppliers, customers and intermediaries and service relations with public institutions.*

4.2 Vital and critical services

In general, vital services are defined as those that are strictly functional to meeting the fundamental liquidity needs of economic agents, any interruption of which, even of the briefest duration, has serious repercussions on their business operations. Critical services are those that, while being of major importance, can nonetheless tolerate a longer interruption of operations without grave damage.

The operators of the systems involved will identify the components that correspond to vital services and to critical services. They will consider all the elements needed to determine the level of business continuity attained and to bring it up to the level desired by preventive measures and contingency plans.

For each activity, the components and resources involved in the provision of the service must be identified (e.g., support procedures, the staff assigned, the logistical structures, the technological infrastructure, the telecommunications equipment and systems, the applications and system software, skills, etc.).

The analysis must involve at least the following points:

- *For each vital or critical service, in accord with the authorities, the company establishes the objective parameters to monitor and their top expected values (e.g., maximum time to renewed operation in recovery configuration, percentage of availability).*
- *Processes relating to these services generally use resources that are highly available. Normally the technology permits "hot" data recovery, meaning the creation of constantly updated backup files or technological systems with malfunction tolerance (e.g., with duplicate equipment).*
- *The people responsible for each process help determine the high availability characteristics in measurable terms (e.g., maximum interruption time) for all relevant resources. They help to develop measures of continuity on the basis of the business continuity plan.*
- *For vital services, the technology must be highly dependable and properly adapted to the latest developments.*
- *Explicit consideration must be given to the danger of data loss, and the procedures and time for recovery must be specified.*

4.3 The content and management of the plan

The business continuity plan must document, in sufficient detail, all the activities relating to the declaration of a state of crisis, the organization and procedures to follow in such a situation, the path to the resumption of operations, the safeguards introduced and choices made as a result of analysis, and the modalities of external communication.

The plan will specify the data-processing sites, spaces and equipment for the staff deployed. It will indicate the modality and frequency of production of copies of production files, set the rules and timing for their storage, describe the procedures for restoration of files in the systems located in alternative sites.

The frequency of copies depends on the volume of business and the importance of data integrity for continuity of the procedure. Support files are normally duplicated continuously. Precautions are taken to make sure that electronic copies are stored in physically secure sites. The standards for file alignment are defined.

The plan determines the modalities of communication with the Supervisory Authorities, with other market participants, with other authorities, with the media and with the public.

The supervised entities that use outside suppliers for the realization of the plan must take due precautions to ensure that the capability for adequate service provision is never lacking.

The contract with the supplier must permit the operator to use the recovery centre for prolonged periods, until the primary site has been restored to full operation.

The plan will identify essential staff to ensure the continuity of relevant activities and instruct them as to the sites to go to and the activities to undertake in case of emergency. The staff involved will be given a constantly updated manual with all needed instructions for cases of crisis.

Every unit within the organization must designate an emergency head. When the technological or organizational configuration of the service is modified, appropriate changes to the business continuity plan must be made and verified.

The plan designates alternative staff to use in case of non-availability of those normally envisaged. Staff will be trained for emergency measures. Consideration should be given to the

possibility of organization involving a number of different shifts and/or sites, as well as mobile units for remote services.

The depth and frequency of periodic tests will be in proportion to the risks and to the importance of the processes. Tests should involve all the persons and organizations potentially affected.

The plan must be regularly tested, at least once a year, and the test conditions must be as close as possible to real situations.

Testing of proper functioning of the continuity plan must be complete, the results must be documented and reported to top management, to the operational units and to the audit function, as well as to the Supervisory Authorities. Corrective measures must be undertaken promptly to remedy any shortcomings detected in the course of testing.

4.4 Outsourcing and relations with utilities

The outsourcing of activities in connection with vital or critical services does not relieve the service operator of responsibility for the maintenance of business continuity. Where software management and/or hardware is outsourced, in the course of the analytical work towards the preparation of the continuity plan the service operator must acquire full familiarity with the outsourced system and its organization. The operational continuity plan of the service operator must cover all aspects involving the elements outsourced. The plan is prepared and finalized under the full responsibility of the service operator.

Where an outside supplier is not compliant with the requirements of the continuity plan and adequate responses in this regard via contract cannot be expected (e.g., for utilities), the system operator must prepare alternative sources of supply.

The requirements of these guidelines also apply where the operator has assigned part or all of the service to an outside company.

Contracts with suppliers must specify guaranteed service levels in case of emergency and identify solutions that satisfy the operator's needs, consistent with the risk analysis scenario and operational objectives.

For supply contracts for utilities, the operator must acquire the supplier's emergency plans or obtain satisfactory information to determine the quality of the emergency measures envisaged and develop coordinated solutions for business continuity. If the requisites are not met, the operator will procure secondary suppliers for the same services or prepare independent sources for self-sufficiency (such as auxiliary generators or battery pools, duplicate telephone lines).

4.5 Agreements with other organizations

To attain the intermediate operational objectives for business continuity, companies will prepare a complete mapping of their dependency on third parties, with special consideration for service suppliers, especially in the financial sector, and the users and members of their own services, on whom the success of actions may depend.

For each such dependency, the operator company will analyze the possible impact on the dependability and regular operation of its own services, highlighting the essential organizations and nodes. With each of these parties the operator will prepare cooperation agreements designed to respond to these objectives, prompt collaboration in case of emergency, the procedures and

instruments for disaster management. The contractually established procedures will be tested as part of the emergency testing programme.

The map of dependencies, the list of critical infrastructures and the related agreements will be promptly notified to the Supervisory Authorities.

Agreements with other important institutions within the financial system will set mutually guaranteed "service levels" and identify solutions consistent with operational objectives. Such agreements will give each operator sufficient information to evaluate the quality of the final result.

4.6 Secondary sites

The location, configuration and management of production sites and operational continuity sites (recovery centres) must be such as to minimize the probability of a simultaneous blockage of activity in the centres. Operators must evaluate the possibility of additional sites for the recovery of the most important data and of the applications software for service management.

Impact analysis must consider the consequences for system operations of major calamities such as natural disasters (floods, earthquakes), air crashes and terrorist attacks. The company's top management must guarantee, based on adequate analysis, that the primary and secondary sites have different risk profiles and must conduct a careful evaluation of the residual risk of simultaneous blockage of the two sites.

The use of infrastructures (such as telecommunications and electricity) must be diversified by site. The availability of viable alternatives to essential public services (such as transport) must be verified. The usefulness of keeping a third copy of production files, stored with appropriate safeguards, should be evaluated.

5. Relations with the Authorities and deadline for implementation

To comply with these guidelines the relevant companies will submit a planning document to the Supervisory Authorities by the end of 2004. The measures provided for in that document must be completed by the end of 2006. The state of advancement of the plan must be reported every six months. Companies must in any case report all relevant circumstances that may affect attainment of the objectives.