CODISE

Cyber Poison 2014

Business continuity simulation for the Italian financial marketplace

17 October 2014

Introduction

The sixth Italian national business continuity simulation was carried out on 17 October 2014; in addition to the Bank of Italy and Consob, the other systemically important participants in the Italian financial marketplace took part: Banco Posta, Cassa Compensazione e Garanzia, e-MID, Equens, ICBPI, ICCREA, Intesa San Paolo, Monte dei Paschi di Siena, Monte Titoli, MTS, SIA, and Unicredit. Given the scenario for the simulation, Borsa Italiana was also invited to participate.

In the exercise, the participating institutions all operated at their own facilities; the relevant regulations required the presence of their internal auditors. The total resources committed amounted to more than 600 man-days.

Objectives

The exercise served to test the adaptation of the systemically important operators to the new business continuity requirements and the CODISE guidelines with reference to:

- the management of extremely adverse situations, i.e. scenarios of extensive crisis and prolonged blockage of the financial market infrastructures, requiring resort to procedures that are not closely integrated into regular corporate processes to serve their own and their customers' liquidity needs;
- the escalation measures, the process for declaration and management of the state of crisis, integration with the incident management process;
- the management of communications with important counterparties;
- the recovery from the emergency, with special attention to damage assessment, the management of service restoration operations, and testing the operability of the services restored.

The characteristics of the simulation

The exercise did not require technological recovery, it did not involve production data or operating procedures of the institutions involved, and it did not require the availability of special technological environments for the trial of financial services, save the communications apparatus, and it did not involve any institutions outside CODISE.

The simulation was conducted in three sessions: morning (08:00 – 13:00), dedicated to crisis management; afternoon (15:00 -16:30), focusing on the return to normal operations; and evening (17:30 – 18:30), with a discussion, coordinated by Mr. Fabio Panetta, Deputy Governor of the Bank of Italy, on how the exercise had gone and possible areas for improvement.

The scenario

The exercise, entitled "Cyber Poison 2014" and designed by a CODISE task force, assumed a very large-scale event with a number of different repercussions on the single participant institutions. As in a real-world event, the various participants were involved with differing degrees of intensity.

Cyber Poison 2014, using the "fast-time" technique, simulated in just one day the activities of four days in June 2014, taking as reference the actual financial data for those days. It simulated a context

of high market volatility, including critical days in terms of liquidity given the falling due of tax obligations and the settlement of main refinancing operations.

The scenario was designed to test the financial system's resilience to a large-scale cyber-attack – an alteration of the software of two critical service providers with an impact on data integrity at banks and market infrastructures – whose impact was propagated rapidly to the entire Italian financial system and its users (consumers, firms, general government bodies). The scenario called for significant spillovers also on foreign markets, but these were not involved in the test.

The results

The exercise was characterized by the strong involvement of all the systemically important institutions; it tested – with all the limits of a simulation – the ability of the financial system to handle a large-scale operational crisis. It verified the processes for communication and coordination within the sector and enabled systemically important operators to test the adequacy of their countermeasures with respect to regulatory requirements in the case of severe operational crisis, in particular against a massive cyber-attack.

As in any exercise, some schematization of reality was needed in order to compress into just a few hours of simulation events that would have occurred over the course of four days. Some major areas where improvement is needed were detected, and action in their regard will be taken over the coming months.

The results were observed and recorded by the Bank of Italy during the exercise, discussed in the evening session, picked up by the participants in their feedback forms, and analysed by the participating banks' internal audit units. Overall, the outcome was positive, and all the participants found the simulation to have been highly useful. In particular, they were especially satisfied with the test of the mechanisms of escalation up the management hierarchy.

The exercise highlighted a good number of points for reflection on possible improvements to the financial system, the procedures and functions of CODISE's technical equipment, the characteristics of the simulation itself, and the systemically important operators' satisfaction of the new business continuity requirements. The most important points are set forth below.

Points relating to the financial system

- Further study will be given to the issue of the maximum period of time that the financial system can continue to operate using TARGET2 contingency payments before the impact becomes unsustainable.
- The systemically important operators may want to assess the possibility of adjusting their collateral management methods to reduce dependence on single infrastructures.
- More detailed verification of the State Treasury procedures in the case of serious operating crisis is needed.
- More thorough analysis is required, from the systemic standpoint, of the crisis management plans in place at the Bank of Italy and at the commercial banks for cash management.

Adaptation to business continuity requirements

- For better system resilience, there will be a review of the criteria for designation of institutions as systemically important intermediaries.

Characteristics of the simulation

- In some instances the "fast-time" technique resulted in a divergence of the passage of time between the different corporate functions, making it hard to maintain a unified overview of

the crisis. There should be an assessment of possible scenarios that are less diluted in time or of that allow a longer time for the exercise, possibly holding it on non-working days.
- Scenario design will have to pay more attention to checking the mechanisms for the coordination of communications to the public and to the authorities.
- Future exercises might well focus not just on the organizational but also on the technological issues connected with the handling of cyber emergencies.

Prospects

The positive results of the Cyber Poison 2014 simulation confirm the validity of the CODISE procedures for cooperation between systemically important operators (banks, market infrastructures, service providers) and the authorities.

In the medium term the simulations can be made more effective by designing scenarios with a cross-border dimension and/or simultaneous disaster recovery tests, with operations conducted at back-up production facilities for a week or more.