

Box 19 Business continuity in payment systems

The rapid recovery and resumption of payment systems, in particular for systemically important payment systems (SIPS), is a key prerequisite for the resilience of the financial system to adverse shocks. In light of the new risks posed by the post 11 September environment, a number of efforts are currently under way worldwide to improve the recovery and resumption capabilities of payment systems. The objective is to provide guidance to system operators so that sufficiently robust and consistent levels of resilience are achieved across those systems. From a practical perspective, the evolution of the oversight policy for payment systems will consist of a further specification of Core Principle VII. This Principle states that *“the system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing”*, but contains implementation guidelines that only cover business continuity arrangements in a rather generic way.

The main elements of business continuity plans that should contribute to ensuring a level of resilience of payment systems consistent with the objective set out by CP VII are the following:

1. Systems should have a well-defined business continuity strategy, which should be endorsed by senior level management. Critical functions should be identified and processes within those functions categorised according to their criticality. Business continuity objectives should aim at the recovery and resumption of the critical functions within the same settlement day.
2. Business continuity plans should envisage a variety of plausible scenarios, including major, wide area disasters. Systems should have a secondary site and the latter's dependency on the same critical infrastructure components used by the primary site should be the minimum compatible with the stated recovery objectives under the scenarios considered. Well-structured crisis management teams and formal procedures to manage crises should be set up.
3. The effectiveness of the business continuity plans needs to be ensured through regular testing of each aspect of the plan. Performing whole days of live operations from the backup site should be considered, and the latter should also be periodically tested with the backup facilities of major participants. Participation of systems in industry-wide testing could be implemented. The business continuity plans should be periodically updated and their disclosure by system operators considered.