SIMONT
BRAUN

31 March 2020

Covid-19 & Banks: Emergency Response and Sound Management

The health crisis caused by Covid-19 and the economic and social consequences it has for banks oblige these financial institutions to inform their regulator of the specific measures, both internal and external, that they implement to address the situation.

Business Continuity – Regulatory Context

Given their essential role in the economic and financial system, banks are legally required to pay particular attention to the risks that are associated with a potential halt or slowdown of their activities.

This is an illustration of the banks' more general obligation to have at all times adequate measures to ensure the maintenance or rapid restoration of their critical functions (Article 21, § 1st, 9°, of the Banking Act of 24 April 2014). This requirement results from the need for credit institutions to have a sound and prudent management in place.

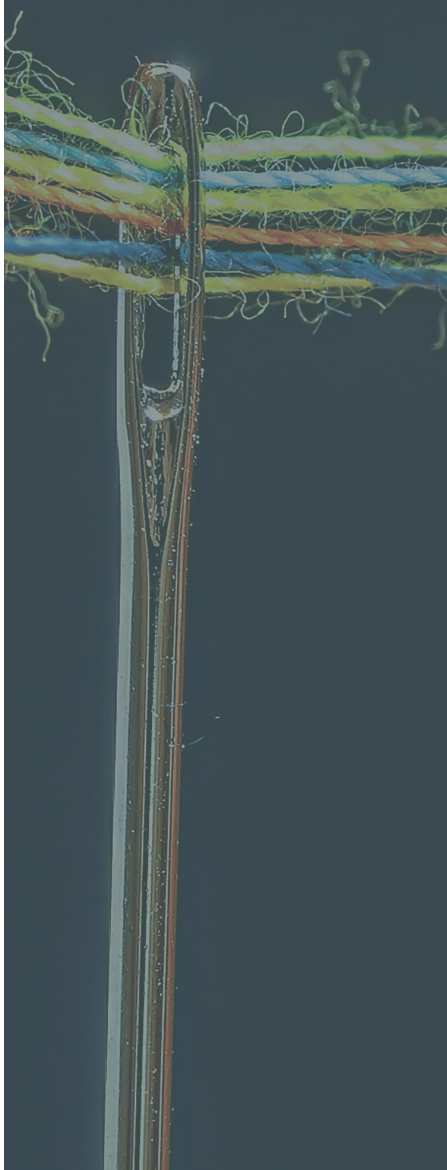
1. Contingency Plan

This obligation of continuity is reflected in the contingency, business continuity and recovery plan. This plan must be established by all banks on an annual basis under the responsibility of their Board of Directors. The contingency plan must demonstrate (and convince the supervisors) that the banks have the capacity to limit the operational, financial and legal consequences that would result from a disaster (we usually think of a fire at the head office, but also a severe computer bug, a terrorist attack or, in this case, a health crisis), or result from a prolonged unavailability of its resources leading to difficulties in ensuring the institution's operations or, in the most serious cases, forcing the institution to interrupt its activities.

As risks are likely to change and evolve, credit institutions must of course regularly test their contingency plans to be able, in a given context, to document and analyse the shortcomings or errors that emerge during testing, and then update their plans accordingly.

2. Preliminary risk analysis

The development and drafting of this contingency plan require banks to have first carried out a detailed analysis of their exposure to serious business disruptions and to have assessed how to address them, both quantitatively and qualitatively. It is the only manner for banks to be able



to define their priorities and objectives should an incident occur.

The spectrum of risks that can hinder or even prevent the continuity of an institution's activities is obviously very broad and depends above all on the activities carried out by the bank. The risks incurred by a private bank differ, at least in part, from those incurred by a bank whose main activity consists in granting mortgage loans to private individuals or by an institution specialising in export financing.

Covid-19: Emergency and continuity measures

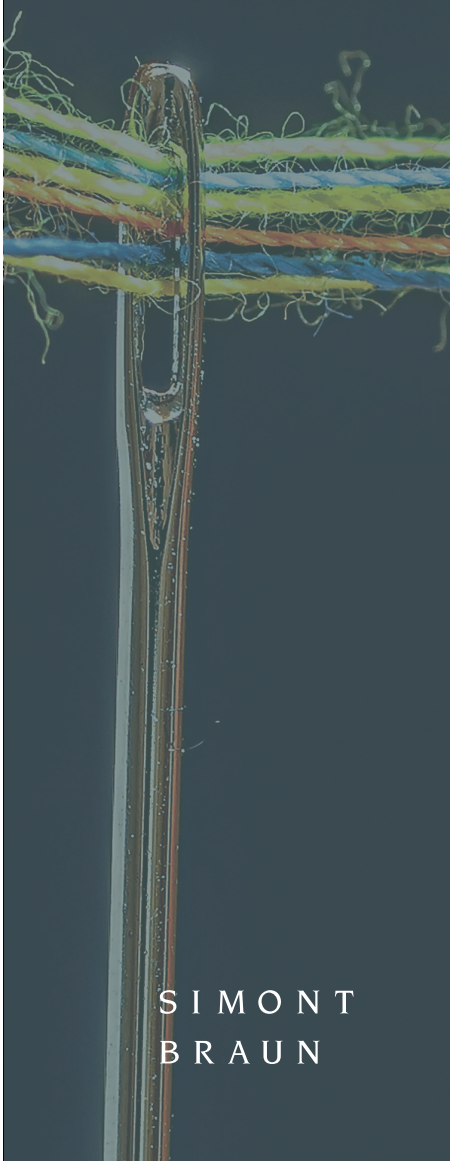
The Covid-19 crisis is a severe test of the banks' obligation of continuity and the accompanying duty of vigilance.

It is the duty of each bank to urgently establish and maintain, throughout the Covid-19 crisis, the necessary measures to ensure the continuity of their activities while protecting their staff and complying with the government measures.

The scenario of a health crisis of this magnitude and its important economic consequences was unlikely to be included in the banks' contingency plans. Nevertheless, in theory, credit institutions must have appropriate tools to face it.

In practical terms, and without going into the details of each institution's particularities, the following emergency measures are examples of what banks can do to deal with the current crisis – from a regulatory standpoint:

- Raising staff awareness and implementing concrete measures to avoid the spread of the virus (teleworking, shift of teams, reduced flex-office, closure of branches, etc.);
- Implementing reliable alternatives for customer communication;
- Increasing IT capacity to cope with remote working;
- Coordinating critical processes, resources as well as critical staff and their back-ups;
- Reinforced assessment by the compliance of cyber-attack scenarios and implementation by IT of the measures internally (monitoring of operations) and externally (communication to customers). Risks of fraud such as phishing, identity theft, etc. increase in times of crisis;
- Additional requirements for subcontractors performing critical functions (outsourcing). This is the case, for example, if customer data is stored in the cloud;
- Setting up of a crisis committee that assesses the situation on a daily basis;
- Communication of the measures implemented to the Board of Directors and possible convening of the risk committee and/or an exceptional audit committee;
- Regular reporting to the competent financial supervisors (e.g. the National Bank of Belgium) on the implemented measures;
- Assessment and possible adaptation of the emergency plan. This assessment is normally made on an annual basis, but it should also be carried out when the emergency plan is to be implemented.



SIMONT
BRAUN

Conclusion

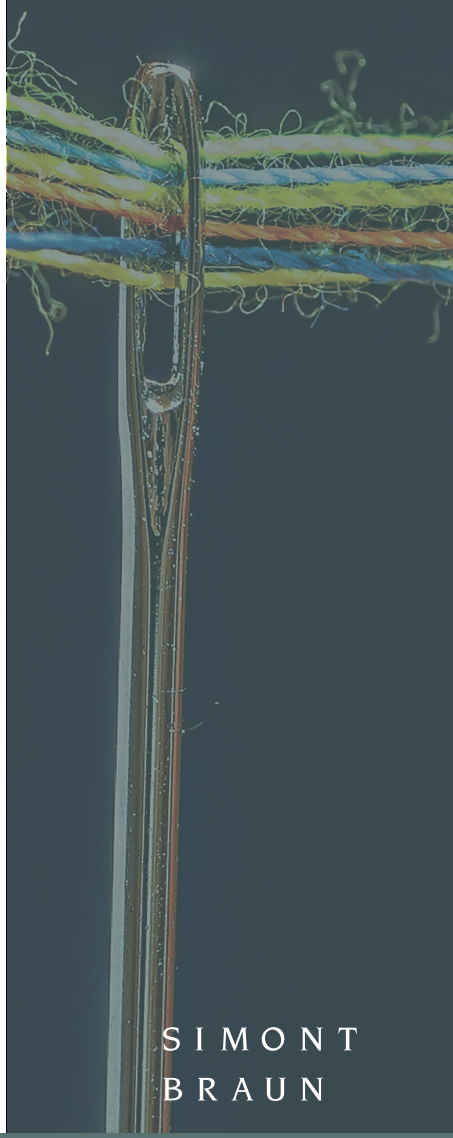
Banks are subject to very burdensome and stringent regulatory requirements. These include the detailed assessment of their risks and the implementation of necessary measures to address the risks identified. This obligation is complex because the regulator requires a risk-based approach that is both concrete and detailed.

However, it is in days like these, when a concrete risk arises that the full usefulness of these regulatory requirements becomes apparent. Afterwards, useful lessons will most probably be learned as to the effectiveness of the current regulatory framework in this respect, and possible modifications can be proposed.

* * *

For any question or request for assistance, please contact:

Catherine Houssa - cho@simontbraun.eu
Philippe De Prez - phde@simontbraun.eu



SIMONT
BRAUN