Thematic article: Emerging practices for pandemic resilience

Filip Caron

Since the outbreak of SARS-CoV-2 in late 2019, financial market infrastructures (FMIs) have increasingly faced adverse effects as the infectious disease outbreak rapidly gained pandemic proportions. Both the industry and authorities have been focusing on the appropriate management of risks related to resource (people, processes, technology, facilities and information) failure.

Existing business continuity plans and working-from-home (WFH) arrangements have been successfully leveraged to guarantee operational resilience in the short term. However, a pandemic may further complicate an operator's ability to respond to additional operational stress events.

Pandemic recovery plans that enable FMIs to continue providing robust platforms and operations consider challenges that deviate from those encountered in more stereotypical business continuity scenarios. Unlike incidents caused by natural disasters, infrastructure failures or cyber attacks, the pandemic scenario needs to consider prolonged and potentially recurring periods of widespread operational stress as a pandemic is not a one-off incident impacting a specific location.

Belgian FMIs, payment systems and critical service providers have continued to provide reliable services to their participants and customers during the first wave of the pandemic. This article aims to identify both best and emerging pandemic resilience practices, but also looks beyond coping with the direct impact of the pandemic.

Emerging practices for immediate response

Over the course of January 2020, the risk of a widespread and potentially global pandemic became increasingly real. As a result, major FMIs started putting the initial stages of their pandemic recovery plans into practice.

A pandemic recovery plan typically defines which sets of risk-mitigating measures need to be employed in different pandemic phases (e.g. interpandemic phase, alert phase, pandemic phase and transition phase as defined by the World Health Organisation). As the global average of cases increases – as well as the direct impact for the infrastructure, system or service provider defined in terms of absenteeism or number of infections – executive and steering committees decide to gradually roll out the pandemic recovery plan and implement risk-mitigating measures.

Ensuring the availability of employees critical to core operations and service provisioning has been a top concern for continuity and recovery planning. There are several reasons for wider unavailability of key employees, including sickness, issues with remote work arrangements, individual challenges like childcare and mental health concerns.

Additionally, FMIs need to comply with the pandemic guidelines issued by the domestic and local authorities. As lockdowns became the norm in most jurisdictions around the globe, these guidelines mandated extensive WFH arrangements with limited exceptions for critical workers.

Emerging and best practices *for the initial pandemic phases*, typically characterised by greater vigilance as the virus has been identified in humans and an epidemic develops in at least one remote jurisdiction:

- **Establishing an appropriate governance team:** Managing implementation of the pandemic recovery plan should be the responsibility of a steering committee composed of executives and key experts. Additionally, separate task forces may be established to address specific business continuity, technical, legal, human resources, communication and health related challenges;

- **Guaranteeing staff safety:** Ensuring the welfare and safety of employees should be the top priority. Education and awareness campaigns are a natural starting point for raising staff safety and reducing the likelihood of infection. Office health supplies including hand sanitisers and personal protection equipment like face masks and gloves should be acquired and distributed. FMIs should aim at reducing staff interaction by avoiding large meetings and extending working hours to reduce crowding in their facilities. Employees who return from countries or regions badly affected by coronavirus or become ill should self-isolate. Furthermore, FMIs should review visitor procedures and restrict business travel;

- **Acknowledging critical services and roles:** Identifying services (e.g. settlement processes) that must be guaranteed throughout the pandemic, as well as the roles needed to provide these services. Scenario analysis based on varying impact on absenteeism provides better insight in the adverse effect and additional mitigating actions. Examples of these additional mitigating actions include explicitly defining redundant teams for critical roles and identifying individuals that could be rapidly cross-trained when needed. The latter requires up-to-date and readily-available procedures, manuals and handbooks;

- **Preparing for WFH arrangements:** Assessing the ability to timely activate long-term and large-scale remote working. FMIs should review existing WFH arrangements for critical employees; test the capacity and scalability of IT infrastructure (including authentication mechanisms) supporting the WFH arrangements; and review the control framework to ensure effective and secure WFH arrangements;

- **Reviewing incident response processes:** Evaluating different incident scenarios to determine the ability to timely and effectively respond to (operational) incidents. FMIs should plan adequately for scenarios that could not be managed remotely. This includes ensuring that additional staff can physically enter the FMIs' facilities, offering safe and timely transport options and minimising the likelihood of infection on the premises;

- **Reviewing succession plans:** Establishing the processes and triggers to delegate authority when senior managers and executives become unavailable. Clear upfront communication should reduce the potential risk of disorientation.

Additional measures taken *as the number of infections rapidly increases and a pandemic outbreak becomes reality* include:

- **Enacting WFH arrangements:** Activating long-term and large-scale WFH arrangements, while ensuring that critical workers obtain permits – in line with authorities' guidelines – to access the technical infrastructure if needed;

- **Monitoring the physical and mental health of employees:** Tracking sickness and unavailability among employees, which will guide the implementation of additional measures of the recovery plan. Furthermore, isolation and extreme stress due to increasing responsibilities at work or at home may result in declining motivation or even burn-out among staff members. Therefore, human resource management should focus

on identifying early signs of deteriorating mental health and proactively provide tools to further minimise unavailability of key employees.

Preparing for continued and additional operational stress

Since the first quarter of 2020, Belgian FMIs and their participants have been operating under exceptional circumstances. However, it is important for FMIs to maintain adequate operational resilience as stipulated in the CPMI-IOSCO's Principles for Financial Market Infrastructures and Guidelines on Cyber Resilience, under these rapidly evolving non-business-as-usual circumstances.

Additional operational stress events may result from physical infrastructure failures, cyber and information security incidents and payment and settlement delays. A massive switch to WFH arrangements has stimulated the creativity of cyber attackers in developing COVID-19-related attack vectors (e.g. specific phishing campaigns), while the number of endpoints may have increased significantly. Moreover, as control frameworks might have been revised to support WFH arrangements (e.g. missing physical access controls and secure document disposal), these endpoints may be more attractive for cyber attackers.

Some FMIs have been confronted with unprecedented transaction volumes. Transaction volumes observed at these FMIs at the beginning of the European lockdowns required an upscaling of the capacity of information systems. In a limited number of cases, settlement and risk management processes have been impacted and operating hours needed to be extended.

Authorities have requested FMIs and other incumbents of the financial services industry to critically review their business continuity plans (including the pandemic recovery plan) in light of the current operational environment. FMIs' executives and senior managers are responsible for designing and updating their pandemic recovery plan, as well as translating the plan into concrete policies, processes and procedures. Boards of directors are responsible for overseeing the establishment and evolution of the pandemic recovery plan, as well as reviewing the related resource investment and testing.

But an FMI's response to an additional operational stress event may not only depend on its own ability to handle incidents, both remotely as on premises. FMIs may depend heavily on critical service providers as well as IT infrastructure and technology solution providers. The status of critical infrastructure which SWIFT has obtained in all jurisdictions critical to its messaging service provisioning grants crucial exemption in times of lockdown (e.g. a limited number of critical staff are allowed to travel and access critical facilities). Not obtaining critical infrastructure status may significantly impact the IT infrastructure and technology solution providers' ability to respond in a timely manner to an operational incident and could have knock-on effects on FMIs' operational resilience.

The following emerging and best practices in updating business continuity and pandemic recovery plans have been observed:

- **Identifying and interacting with critical third parties:** Obtaining in-depth insight into the business continuity provisions of critical providers is crucial for determining the ability to guarantee critical service provisioning during the pandemic. Furthermore, whenever an FMI cannot gain reasonable assurance on the adequacy or effectiveness of service providers' plans, it should prepare contingency plans for shifting to alternate providers;

- **Re-evaluating the pandemic extreme risk scenario:** Assessing the extent to which business continuity plans address the pandemic extreme scenario, as well as the ability to implement, scale and sustain additional

measures in good time. For example, traditional business continuity plans typically leverage alternate sites to deal with natural disasters or other emergencies. However, during pandemics, FMIs may be faced with shortages of available staff to relocate and – as is currently observed with the COVID-19 pandemic – the alternate sites may be severely impacted as well;

- **Finetuning the metrics and triggers of the pandemic recovery plan:** Developing detailed monitoring systems to more accurately capture the progression of viral outbreaks and specify triggering events. In addition to traditional news sources, a variety of alternative yet highly reliable sources have emerged during the COVID-19 pandemic, e.g. the detailed and integrated statistics provided as well as the critical trend analyses by Johns Hopkins University. These additional data points should enable more detailed implementation of mitigating measures, as well as a closely controlled return to business as usual, although a business-as-usual scenario may only be achieved after a vaccine has been found;

- **Re-assessing the cyber threat level and controls:** Identifying emerging weakness due to increasing security backlogs or relaxed controls to enable WFH arrangements, as well as evolving cyber threat landscapes as attackers take advantage of general disorientation and confusion (e.g. in phishing mails). FMIs could enhance monitoring capabilities for their critical information systems which act as (partially) compensating controls to timely detect a cyber attack. Furthermore, FMIs should continue raising awareness of cyber security risks. Similarly, there have been indications of increased targeting of participants' operated endpoints.

The COVID-19 pandemic has resulted in extended periods of uncertainty and operational stress, potentially impacting available critical resources and other project inputs like stakeholder interaction. FMIs may face significant project delivery risks and may need to reprioritise projects. Embarking on numerous new projects in combination with significant pre-COVID-19 technology renewal may result in excessive demands on critical resources and derail strategic responses to market developmentss.

Emerging practices include:

- **Assessing impact of the pandemic on project delivery:** Identifying the potential impact of a pandemic on the availability of supporting resources and processes (including training and dependency management). Reviewing the demands on key resources to enhance security and efficiency for WFH arrangements, including demands related to legal and regulatory requirements;

- **Coordinating with key stakeholders:** Reviewing the capacity of stakeholders both internal and external to contribute to key projects, e.g. ability to review prototypes and engage with agile software development teams or availability for resilience testing. FMIs have also allowed their participants additional time to meet less critical requirements;

- **Assessing risks induced by the pandemic and formulate risk responses:** Establishing appropriate risk identification and assessment processes to review proposed delays and request formal risk acceptance by management where needed. The Board of Directors' risk committees are responsible for the oversight of these risk management practices.

Planning for the resumption of onsite working

At the end of the second quarter of 2020, the average daily number of new cases fell sharply in Europe, as the transition phase of the pandemic was entered. FMIs started considering reopening facilities for non-critical staff in a gradual and cautious manner.

The resumption of onsite working involves a series of precautionary measures, as the threat of a second and subsequent waves remains realistic:

- **Gauging the comfort level of employees:** Engaging with employees to understand their willingness and ability to return to the office. Several important challenges have been identified in this context, notably related to commuting (because employees are keen to avoid public transport) or to a lack of appropriate childcare. Most FMIs anticipated that WFH would remain standard practice for most employees, at least until the end of the third quarter of 2020. As a result, FMIs continue to invest in productivity training for remote collaboration;

- **Phasing in the return to onsite working:** Working with split teams to ensure back-up for critical functions. Establish work schemes that alternate onsite working and WFH. Reallocate employees across different sites to mitigate undue risks in any one location. FMIs may also start analysing requests to restart non-critical services that require physical presence and identify the employees supporting these functions.

- **Ensuring physical workspace safety:** Deep cleaning and implementing other infection control measures for physical facilities. Redesign foot traffic flows to avoid congestion and enable appropriate social distancing. Establish symptom monitoring controls like temperature checks, which although not fully watertight may identify potentially infected employees. Ban large meetings with personal attendance. Continue pandemic awareness campaigns;

- **Redesigning of processes and workflows:** Reducing the number of physical handovers to the absolute minimum and automate critical processes wherever possible.

Actions by authorities

Belgian supervisors and overseers of FMIs, payment systems and critical service providers have been reviewing the appropriateness of the pandemic recovery plans and continue to closely monitor any adjustments made in the light of the evolving pandemic risk.

Special attention is being placed on obtaining reasonable assurance on the effectiveness of the different lines of defence during the pandemic. Supervisors and overseers continue to monitor and challenge the appropriateness of risk-mitigating measures, including measures related to the scalability of IT infrastructure, to the ability to respond to incidents and to the improvement of cyber resilience.

The Bank is represented in the CPMI and actively contributes to analyses of the effectiveness of WFH arrangements and operational resilience in times of a pandemic.