MONEYVAL: Typologies Report on AML/CFT Supervision in Times of Crisis

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

András Csúri

AUTHOR

András Csúri

Vienna University of Economics and Business

Published in
2022, Vol. 17(1) eucrim pp 41 – 42
ISSN: 1862-6947
https://eucrim.eu

On 25 January 2022, MONEYVAL published a report that aims to assist authorities in effectively carrying out their supervisory activities as regards anti-money laundering and countering the financing of terrorism (AML/CFT) in times of crisis. The COVID-19 pandemic has created new threats and vulnerabilities to the AML/CFT system. Supervisors have been faced with new challenges, mainly in relation to the proper assessment of risks involved and the communication of appropriate mitigating measures to the obligated entities.

The report is designed as a best-practice paper containing an overview of business continuity measures that supervisors should consider within the context of challenging external factors. It builds on an earlier analysis of AML/CFT trends in MONEYVAL jurisdictions during the COVID crisis (→ eucrim 3/2020, 197-198). The report is mainly based on information collected from supervisors of thirty-one MONEYVAL jurisdictions and from other international actors; furthermore, qualitative data were obtained through follow-up interviews and additional written contributions. The questionnaire focused on risks and challenges, solutions to business continuity and crisis management measures, digitalization and other regulatory adjustments as well as supervisory tools, sanctions, outreach, and international cooperation.

The primary challenge for supervision has been the transition to remote working. The pandemic impacted the working conditions of the supervisory authorities by limiting access to buildings and by limiting the number of staff available to carry out daily tasks. In addition to throttled human resources, technical shortcomings (access to IT support, databases, and information from reporting organisations) were also a problem.

Based on a comparison of the different approaches, the report concludes that early business continuity management in the form of Business Continuity Plans (BCPs) has led to minimal disruption to the functioning of supervisory authorities. The majority of the responding supervisors had BCPs for possible crisis scenarios in place before the pandemic outbreak, but only one country's BCP included a specific pandemic scenario. Some jurisdictions had a BCP that had not yet been finalised or not yet adopted, while one jurisdiction reported that its BCP did not cover AML/CFT supervision.

The BCPs include risk assessment methodologies, detailed governance arrangements, division of responsibilities, and specific measures to be implemented in response to a crisis in order to ensure that business can be continued. It has also proven beneficial to include AML/CFT supervision in such plans. Given the physical

movement constraints and the need to use virtual meetings and other forms of communication, the involvement of IT and internal security departments in the development of BCPs also appears to be a good practice.

There were new protocols implemented to ensure data security, and staff were trained on related issues. Other measures with positive results included the setting up of coordination committees to distribute AML/CFT supervision among several supervisors.

The pandemic has shown that technology is key in crisis situations in which employees cannot return to the office. In order to mitigate the ML/TF risks, supervisors and data organisations have been encouraged to rapidly increase the digitalisation of their core functions in order to maintain operational continuity. Among other things, video conferencing tools enabled the collection of information/documents from reporting entities on ML/TF risks and hybrid on-site and/or off-site supervision. This is also essential in other challenging circumstances, e.g. monitoring entities with limited or no physical presence in a jurisdiction. Supervisors have also used a variety of communication channels, from posting video clips and e-learning materials to online webinars/training.

The most common IT control measures for remote working across various jurisdictions included the following:

- Using secure VPN connections or joining the call using special platforms;
- Limiting and controlling remote access for users of the institution's server or internal network;
- Restricting downloads from remote computers to personal devices;
- Encrypting locally stored data;
- Recording user activity during remote sessions;
- Multi-factor authentication;
- Regular password changes.

Supervisors have developed guidelines and/or regulations to enable reporting entities to use digital identification systems. Furthermore, they have explored the exceptional use of simplified customer due diligence in low-risk scenarios, for reporting entities to onboard clients and to facilitate the delivery of government benefits.

Cross-border cooperation between supervisors could be enhanced by simplifying existing rules and procedures, including data exchange. Existing memoranda of understanding (MoUs) could include specific provisions for assistance in times of crisis and *force majeure*. In the absence of a specific provision, the general rules of the MoUs could allow and/or encourage communication and cooperation by electronic means, where available.

MONEYVAL member states and territories will be invited to provide feed-back on the use and added value of the findings in one year.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union