IMPACT OF COVID-19 RISKS ON SUSTAINABLE DEVELOPMENT OF FINANCIAL ENVIRONMENT

Leyla Magomaeva, Grozny State Oil Technical University Named After Academician M.D. Millionschikova
Olga Razina, ANO Russian Academy of Entrepreneurship

ABSTRACT

The purpose of the present paper is to define the aspects of the development of a complex system of COVID-19 risk management for financial institutions in the context of efforts to build up remote service channels. The study period covers 2019-2020. Data on the largest credit and financial institutions in Russia were used as an empirical basis. In the course of the study, the COSO ERM methodology "Organization risk management – an integrated model" was used, supplemented and expanded by the mechanism for controlling the balancing of customer distribution. A comprehensive analysis of the FATF standards was carried out to identify the COVID-19 risk system, which made it possible to combine the schemes of committing unlawful actions in relation to customers and directly the credit and financial institution itself. The understanding of the reasons and consequences of changes in the economic environment, financial behavior of clients, signs of increased risk concentration, and programs for additional compliance control of COVID-19 risks in the credit and financial sector was expanded. Based on the analysis of scientific and business literature, non-specific risks were identified, a characteristic feature of which is their localization in the field of digital technologies and the remote customer service channels created on their basis. The author's research shows that the attainment of maximum effectiveness in the adopted system of COVID-19 risk identification at a multi-branch financial institution involves the analysis of events and sources down to the level of individual operational and business processes with a subsequent evaluation and prioritisation of potential threats subject to: systematisation of risk indicators and materialisation patterns; identifying the most vulnerable operational and business processes affected by the risk; identifying the methods to control and manage the risk; determining risk concentration levels and its further balancing in the established compliance procedures and internal reporting. Practical results are presented, conclusions are formulated, and proposals are made for the development of promising areas of countering COVID-19 risks for organizations in the credit and financial sector.

Keywords: COVID-19 Risk, Risk Identification and Management System, Financial Institutions, Anti-Money Laundering Efforts, COSO Methodology, Branches, Balancing, Compliance Control, Compliance Report, Risk Concentration.

INTRODUCTION

Currently, the activation of fraud and crime in the financial sphere has become a special concern globally given the wider risk profile associated with the COVID-19 pandemic (Razina, 2017 & 2018).

Citation Information: Magomaeva, L., & Razina, O. (2021). Impact of covid-19 risks on sustainable development of financial environment. *Academy of Strategic Management Journal, 20*(6), 1-8.

Statistical reviews published regularly by the FATF (Financial Action Task Force on Money Laundering)[1] indicate an increasing incidence of fraud, cyber crime, inappropriate or illegitimate use of public funds or international aid in nearly all areas of economic operations.

It should be observed that COVID-19 risks primarily relate to *"external events"* occurring in the external environment and transformed via various operational and business channels used for communications and remote work (Aldasoro et al., 2020a).

Standard operation in major multi-branch lenders and financial companies involves constant structured communication with many territories based on the existing infrastructure and established operating model (Welburn & Strong, 2019; Maas et al., 2016). However, during the COVID-19 pandemic, many financial institutions switched to the remote regime with some of their functions while maintaining standard customer operation in other territories where the epidemiological situation was less adverse and allowed continued office operation, which helped to cut costs on getting around infrastructure limitations (Dingel & Neiman, 2020). However, sticking with the remote customer operations brought them the welcome opportunities to maintain their operational and business functions but also threats resulting from the intensifying operational and cyber risks (Aldasoro et al., 2020b; Curti et al., 2019), which globally meant the biggest compliance risks (Razina, 2017 & 2018) primarily associated with the risk of money laundering and terrorist financing (Crisanto & Prenio, 2020).

Given that, the crucial factor for overcoming the risks related to COVID-19 is the need to establish an internal system of identification of COVID-19 risks for countering financial fraud and crime.

LITERATURE REVIEW

The active adoption of social distancing due to the COVID-19 pandemic has generated strong research interest in studies of digital technologies (Aldasoro et al., 2020b) and contactless customer finance technologies (Curti et al., 2019; Crisanto & Prenio, 2020). Scientific research carried out in recent years on the problems caused by the spread of operational risk (Burov, 2019, Kapitonova & Kapitonova, 2021, Razina & Kosterina, 2015, Magomaeva, 2019b) revealed the characteristic features of COVID-19 factors influenced by the issues of informal employment, job cuts, lack of social guarantees, and declining salaries.

It was back in 1989 that the Financial Action Task Force (FATF) was established by the global community to manage anti-money laundering efforts; Russia has been a member of the organisation since 2003 ((Rosfinmonitoring, n.d.).

Note that the existing FATF standards provide only general guidance for identifying high-risk customers or transactions in the context of the COVID-19 pandemic, while detailed indicators fall within the competence of national anti-money laundering bodies (Pakharev, 2020) including for the formation of a new type of information infrastructure (Magomaeva, 2018 & 2019a).

The practical aim of this study is to build a complex system of managing and identifying COVID-19 risks to limit the potential of the use of financial institutions in the processes of money laundering. The realisation of this aim requires a new methodology for analysing the concentration of suspicious customers and their transactions under the existing compliance procedures.

METHODOLOGY OF ANALYSIS

As far back as the 1970s, in the context of active development of the financial industry in the USA, the rate of corruption and transnational bribery grew, which provided an impulse for reforms of corporate financial law and urgent measures to enhance internal control programmes in corporations (Razina, 2016a, 2016b). In response, the Treadway Commission was formed in 1985, which issued the first *"Report of the National Commission on Fraudulent Financial Information,"* and later on, the Committee of Sponsoring Organizations (COSO) was formed. Today, the COSO ERM methodology *"Enterprise Risk Management — Integrated Framework"* lays out the fundamental standards of risk management for major global companies, helping to identify the most vulnerable operational and business processes, to eliminate incorrect compliance procedures and build the basis of a risk identification system (Rahman & Al-Dhaimesh, 2018).

The COSO framework specifically focuses on the development of target references for operational and business processes to help identify the main risks and obstacles hindering their attainment (Razina, 2016a). Meanwhile, targets should be matched with an assessment of the level of risk, if the target is not determined, neither are risks for such an assessment (Razina, 2016a).

In our view, effective application of this methodology for identifying COVID-19 risks is contingent on addressing the following functions:

(1) Compliance review of COVID-19 risk identification procedures. A COVID-19 risk identification system should target the existing risks pertinent to the operation of the financial institution and potential risks it may be subject to in the long run.

(2) Using quantitative and/or qualitative methods to assess COVID-19 risks. Such risk assessment models can be based on expert assessments. Expert assessment (self-assessment) refers to quantitative and/or qualitative risk assessment based on professional judgement expressed by skilled professionals of the financial institution and/or external experts.

(3) Mapping out the approaches and methods to manage COVID-19 risks and the list of measures to mitigate them.
The following approaches to COVID-19 risk assessment and risk management should apply based on the following principles:

- the bottom-to-top principle in the identification and assessment of (potential and realised) sources, causes and consequences of risk events in the units of the financial institution and operational and business processes.
- the top-to-bottom principle in the assessment of the implications of risk materialisation (direct and indirect losses/costs, impact on the operational outcomes of the financial institution).

(4) Determining target levels of risk concentration. To contain the COVID-19 risk level, individual limits (by specific risks or aggregate risk types) should be set, in absolute and relative terms.

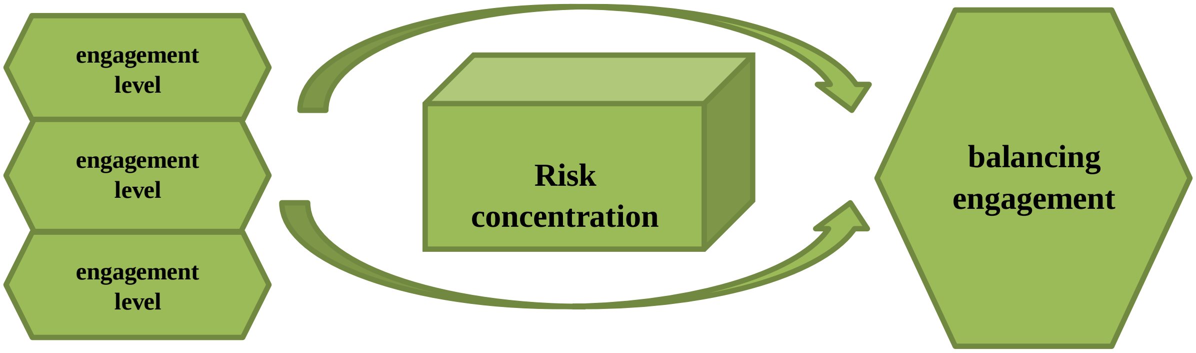
(5) Setting reference values on risk limits and other indicators for triggering COVID-19 risk mitigation measures. Such an assessment of risk limits should involve steps to set up the composition, methodology and target levels of such indicators for launching risk mitigation measures on the specific risk across the units of the financial institution.

(6) Monitoring the level of accepted risks and setting up compliance reporting on their respective levels and risk management performance results. This stage should include the adoption and approval of the forms of regular compliance reporting based on the principles of rationality, accessibility, transparency, completeness, comparability, aggregation, timeliness, integrity.

(7) Enhancing the risk identification system by way of balancing (distribution). Where the above procedure is met, this methodology can be successfully applied for determining risk concentration and further balancing of non-specific risks, such as the COVID-19 risk, which is localised in the domains

of digital technology and remote service channels underpinned by it due to the active development of information resources (Magomaeva, 2017).

In this paper, we propose an improvement of the COSO ERM methodology by expanding the existing composition with a mechanism of balancing customer distribution to neutralise the difference in the engagement levels between different branches according to the following principle: the heavier the problem in the branch, the higher the proportion of customers analysed for any given performance rate of each compliance procedure in the financial institution (Figure 1).



Source: developed by the author

FIGURE 1
THE FRAMEWORK OF BALANCING BRANCH ENGAGEMENT LEVELS IN COVID-19 RISKS IN RISK CONCENTRATION

The customer engagement level (problem profile) of the branch here refers to the ratio of the branch's customers designated to the high-risk group in a controller's compliance report to the total number of the branch's customers included in the report. Compliance procedures are measures to identify such risks during the analysis of customer behaviour, schemes and methods of money laundering or other misconduct.

Each of the analysed indicators of customer engagement levels with COVID-19 risks by the branches should be assigned a rank to help identify the most vulnerable branches of the financial institution. A similar analysis can be further conducted for the operational/business processes with signs of engagement. The number of customers with a high risk rank can be calculated based on the scoring assessment of the customer bracket included in reports for day T-2. The overall number of customers included in the compliance report should be calculated based on the bracket of transactions (performed by corporate and personal customers) uploaded in the uniform information system *"Customer Profile"* for day T-2.

Thus, engagement levels can be calculated for each of the critical control procedures included in the compliance report. That said, the calculations of engagement levels and balancing of compliance control between branches can be performed in an automated mode within the uniform COVID-19 risk identification system; and customer information can be laid out in the *"Customer Profile."*

The following mechanism can be used to balance compliance control.

Customer reduplications are excluded from the reports of the compliance controllers of individual branches in the order of priority, the bigger the branch, the higher the priority.

Engagement levels are calculated for each branch on each critical compliance report.

$$V_{i,j} = \frac{n_{i,j}}{s_j} \tag{1}$$

where:

$V_{i,j}$ is the engagement level of branch j in compliance report i,

$n_{i,j}$ is the number of customers with high risk ranks in report i for branch j,

S_j is the total of branch j included in compliance reports for day T-2.

Next, a reference (minimum) value of engagement levels should be found for each compliance report for all branches:

$$V_{(i)} = min_{1..l} V_i \tag{2}$$

$V_{(i)}$ - reference engagement level for compliance report i among all branches

V_i - minimum engagement level according to compliance report i among all l branches

Accordingly, a balanced number of reference customers can be calculated for each branch to neutralise the engagement level toward the reference value of the compliance report:

$$N_{i,j} = N_{i,j} + N_{i,j} \times \left(V_{i,j} - V_{min(i)}\right) \tag{3}$$

$N_{i,j}$ is the balanced number of reference customers of branch j for compliance report i.

To cut down labour requirements for conducting compliance functions, calculate the performance rate on compliance procedures on day T:

$P = p \times q$, where:

P is the daily performance rate of compliance control;

p is the average daily performance rate of a compliance procedure (retrospective data based on a calendar quarter);

q is the actual number of compliance procedures on day T.

Based on the above assessment, a matrix of high-risk customer numbers should be plotted for a more detailed analysis through the lens of specific territories or branches of the financial institution and individual business/operational processes requiring additional compliance procedures. The following formula should be used to calculate the items of the matrix:

$$\left(\frac{N_{i,j}}{\sum \quad (N_{1,1};N_{k,l})}\right) \times P \tag{4}$$

where:

$N_{i,j}$is the balanced number of reference customers of branch j for business/operational process i.

$\sum \quad \left(N_{1,1}; N_{k,l}\right)$ is the total of reference customers for all k business/operational processes for all l branches within the scope of control

P is the daily performance rate of compliance procedures;

k is the number of critical compliance reports;

l is the number of branches within the scope of compliance control.

The values of the output items in the matrix show the number of customers for each branch through the risk lens of business/operational processes to be analysed by compliance control on day T.

In our view, the enhanced COSO methodology can provide visibility not only into the nature of suspicious transactions conducted by the customers, but also on specific territories and business/operational processes with maximum risk concentration levels on the respective risk at the institution-wide level. The balancing mechanism can be helpful in the distribution of compliance procedures in high risk concentration zones by the engagement levels in specific operational/business processes and transactions. Moreover, this balancing mechanism improves the performance of the COVID-19 risk identification system as a tool to counter fraud and crime in finance.

EMPIRICAL RESULTS

Our study of COVID-19 risk assessment based on the analysis of one of the biggest Russian banks for 2020 indicates that the attainment of targets by individual operational and business processes does not correspond with the existing compliance procedures, as risk event concentration in the most affected branches was due to the increasing volumes of remote banking products and services and branches changing their format of operation amid the mass transition to remote services.

Thus, the practical application of the balancing mechanism of customer distribution to neutralise the difference in engagement levels between branches suggested a conclusion that when risk concentration is identified at the level of an operational or business process, flexible compliance procedures should be adopted based on a given performance rate for such procedures.

DISCUSSION

The results of studies conducted by the IMF (International Monetary Fund, 2020) on the problems of the spread of operational risks under the influence of COVID-19 factors showed that a characteristic feature of their manifestation is the processes and people influencing the decision-making mechanisms, the order of subordination, communication processes, as well as processes associated with people in the conditions of using remote communication channels and interaction. At the same time, the empirical results made it possible to establish that the strongest concentration of COVID-19 risk is manifested in organizations associated with the proliferation of remote banking services, which shape the need for medium- and long-term adoption of flexible compliance control procedures for operational and business processes. The accelerating customer migration does not only bring about intensifying risks but also creates the need for identification of transactions conducted in remote channels, analysis of changes in customer behaviour when using various products or services, development of a compliance framework for new risk assessment and implementation of the existing operational strategy with changed technological practices and new self-service channels across the branch network.

CONCLUSION

The key tasks brought together in the development of a system for managing and identifying COVID-19 risks for anti-money laundering purposes set the potential path of further academic research including the analysis of causal relations between remote service channels and schemes exploited by unscrupulous customers. Such work should be undertaken not only by oversight and control authorities, but also at the level of the members of the financial sector to counter fraud and illegal capital flows.

ACKNOWLEDGMENTS

With the financial support of the Russian Foundation for Basic Research (project No. 20-010-00101 A).

ENDNOTES

1. Note. Inter-governmental body that develops global standards for anti-money laundering efforts and countering terrorist financing (AML/CFT) and monitors compliance across the 228 national AML/CFT systems.

REFERENCES

Rahman, A.A.A.A., & Al-Dhaimesh, O.H.A. (2018). The effect of applying COSO-ERM model on reducing fraudulent financial reporting of commercial banks in Jordan. *Banks & bank systems*, *13*(2), 107-115.

Aldasoro, I., Frost, J., Gambacorta, L., Leach, T., & Whyte, D. (2020). Cyber risk in the financial sector. *SUERF Policy Notes*, (206).

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). *Operational and cyber risks in the financial sector.*

Burov, V. (2019). Practice of the Russian Federation in countering capital flight and money laundering. *Shadow Economy,, 3*(3), 153-164.

Crisanto, J., & Prenio, J. (2020). *Financial crime in times of Covid-19 – AML and cyber resilience measures.*

Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. *Federal Reserve Bank of St Louis, August, mimeo*.

Dingel, J.I., & Neiman, B. (2020). How many jobs can be done at home?. *Journal of Public Economics*, *189*, 104235.

International Monetary Fund. (2020). Central bank operational risk considerations for COVID-19. Retrieved August 20, 2021, from https://www.imf.org/en/Publications/SPROLLs/covid19-special-notes

Kapitonova, N.V., & Kapitonova, A.A. (2021). Trends of the shadow economy in Russia. *Shadow Economy,1*(5).

Maas, K., Schaltegger, S., & Crutzen, N. (2016). Integrating corporate sustainability assessment, management accounting, control, and reporting. *Journal of Cleaner Production*, *136*, 237-248.

Magomaeva, L.R. (2017). Development of fintech companies in conditions of competition with financial mediators for information resources. In *12th International Scientific Conference" Science and Society" SCIEURO* (pp. 98-105).

Magomaeva, L.R. (2018). Monetization of information infrastructure products in the conditions of development of competition in the credit and financial sector. *The European Proceedings of Social & Behavioural Sciences/ Social and Cultural Transformations in the Context of Modern Globalism. (TPHD 2018)*, *308*, 258-262.

Magomaeva, L.R. (2019a). Development of intellectual verification methods for cross-channels for interacting with bank customers. *SCTCMG 2019 International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism», Grozny*, 3544-3552.

Magomaeva, L.R. (2019b). Establishing an integrated bank operational risk management in the context of the development of a new information system. In E.G. Popova & L.R. Magomaeva (Eds.), *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT Studies in Computational Intelligence. Volume 826* (pp. 641-653). Cham: Springer.

Pakharev, A.V. (2020) Problems of countering drug-related money laundering as an element of economic security. *Economic Security*, *3*(3), 363-376.

Razina, O.M. (2016a). Organization of the internal control system in banks using the COSO model. *Accounting in Credit Institutions*, *6*(216), 35-40.

Razina, O.M. (2016b). Possibilities for identifying and reducing the risk of corporate fraud in a bank's internal control system. *Banking,7*(270), 70-73.

Razina, O.M. (2017). Development of a cross-channel information system for combating fraud in a bank. *Banking, 4*(278), 66-71.

Razina, O.M. (2018). The main methods of detecting internal fraud and falsifications in a bank's retail business. *Accounting in Credit Institutions*, *6* (240), 72-78.

Razina, O.M., & Kosterina, T.M. (2015). Innovative instruments of fraud monitoring in internal audits in a bank. *Russian Journal of Innovation Economics, 5*(4), 253-266.

Rosfinmonitoring. (n.d). *Financial Action Task Force, FATF*. Retrieved from https://www.fedsfm.ru/activity/fatf

Welburn, J.W., & Strong, A.M. (2019). Systemic cyber risk and aggregate impacts. *Risk Analysis*..