

A Mixed Approach to Assess Information System Risk, Operational Risk, and Congolese Microfinance Institutions Performance

Alfred Kamate Siviri, Angelus Mafikiri Tsongo, Jean Robert Kala Kamdjoug

Abstract—Well organized digitalization and information systems have been selected as relevant measures to mitigate operational risks within organizations. Unfortunately, information system comes with new threats that can cause severe damage and quick organization lockout. This study aims to measure perceived information system risks and their effects on operational risks within the microfinance institution in D.R. Congo. Also, the factors influencing the operational risk are to be identified, and the link between operational risk with other risks and performance is to be assessed. The study proposes a research model drawn on the combination of Resources-Based-View, dynamic capabilities, the agency theory, the Information System Security Model, and social theories of risk. Therefore, we suggest adopting a mixed methods research with the sole aim of increasing the literature that already exists on perceived operational risk assessment and its link with other risk and performance, with a focus on information system risks.

Keywords—Information system risk, operational risk, microfinance performance, DR Congo.

I. INTRODUCTION

ANY company and especially micro-financial intermediaries, aim at identifying uncertainties and mitigate the risks that could arise from these uncertainties [1]. Risk management has become increasingly important in the course of the operation of microfinance companies due to the lack of risk management and control of risks [2]. Microfinance institutions "hold an important role as a source of funding for the societies and small businesses" [3]. According to [4], uncertainty originates from people and any stakeholder the company interacts with. More than 80% of stakeholders are customers [1], [5]. Microfinance institutions are exposed to several risks, including operational risk and reputational risk every day [4].

In contrast to other financial risks, operational risk is considered a pure risk (only an opportunity for loss) [1]. Such a situation always results in a financial loss for a bank or microfinance institution [1]. The Basel Committee of bank supervision describes "operating risk as the risk of loss arising from entities, insufficient or ineffective internal processes, programs, or external actions" [6]. The fiasco of mitigation and management of operational risks caused the demise of several microfinance institutions in DR Congo. From 2009 to 2015, the

number of viable institutions decreased terribly. It passed from 111 to 76 [7].

The computerization of operational processes has been reputed as one of reasonable control measures for operational risk reduction. In some cases, the software is recommended. As suggested by [8], "investments should also be made to acquire relevant operational risk management software to ensure prompt identification, analysis, and reporting of risk events for prompt management information and decision making". To escape from the hecatomb, many micro-financial institutions have seriously invested in acquiring technological equipment, software, and staff training. They have turned more force to the purchase of the most powerful software. The situation did not prevent some of these structures from bankruptcy. Unfortunately, new types of risks due to digitization occur [9], [10]. IT innovation comes with its risks, which are too little explored in the literature. These risks include information system inadequate organization, information system functioning default, and information system lacking security [11]. In most organizations, especially microfinance institutions, information system risks are still so little known. As a result, their magnitudes are uncontrolled. Also, it is almost impossible to propose mitigating measures.

This study aims at measuring the human perception of information system risks and their link with operational risk based on the information system security maturity model and explore factors behind the microfinance industries' operational risk. The relationship between operational risks, credit risk and reputational risk, and microfinance performance is to be assessed.

The rest of this paper comprehends: Section II the Theoretical background, Section III Hypotheses Development and Research model, Section IV Methodology, and Section V Expected Contributions.

II. THEORETICAL BACKGROUND

This study is built on the combination of five main theories, including the Resources-Based-View, RBV (1), dynamic capabilities, DC (2), the agency theory, AT (3), the Information System Security Model, ISSM (4), and Social Theories of Risk, STR (5).

Alfred Kamate Siviri is with the Catholic University of Graben, High Education college of Muhangi/Butembo, DRC (corresponding author, phone: 00243813142092; e-mail: sivirialfred@gmail.com).

Angelus Mafikiri Tsongo is with the Catholic University of Graben (e-mail: tsongoa@yahoo.fr).

Jean-Robert Kala Kamdjoug is with the Catholic University of Central Africa (e-mail: jrkala@gmail.com).

A. Resource-Based View

Called "Resource-based view" (RBV) in the beginning, this framework became "Resource-based Theory" (RBT) [12]. It holds that business process resources are a subset that contributes to a company's competitive advantage. According to [13], resource theory is one of the strategic management theories that describes how firms gain "competitive advantage by configuring their resources so that they become (1) scarce, (2) difficult to imitate, and (3) difficult to replace." Besides, this theory emphasizes the link between critical resources and business performance.

B. Dynamic Capabilities

Teece et al. [14] define DC as "the ability to integrate, build, and reconfigure internal and external competencies to deal with rapidly changing environments". The theory of dynamic capabilities appears as the result of reproaches to resource-based vision. Indeed, the resource-based vision has been criticized because it ignores all resource-related factors. The RBT assumes that resources "exist". Thus, while DC emphasize the choice of resources or the selection of appropriate resources, DC emphasize the development and renewal of resources. In this perspective, [15] stated that DC complement the notion of resource-based enterprise vision. Based on the theory of firm evolution [16], DC argue that firms should not develop routine capabilities.

C. The Agency Theory

AT emerged in 1960 from an economic perspective to share risk between individuals and groups [17], [18]. This theory addresses the ubiquitous agency relationship, in which one part, the principal, delegates work to another (the agent), who does the work. Resolving problems that may arise in agency relationships is linked to the AT [19]. Abdullah and Valentine [20] concluded that AT could be applied wherever there is a separation to align managers' objectives with those of the owners. Moreover, [21] presents AT as a theory that seeks to explain the various organizational forms as a conflict resolution mode—making a clear distinction between two types of major actors, the principal, and the agent, its interests.

D. Information System Security Model (ISSM)

Information System Security Research Model (ISSRM) is a practitioner-oriented methodological tool [22]. It helps organizations make cost-effective decisions related to information systems' security [22]. Based on a well-structured process, the use of ISSRM reduces losses caused by security weaknesses of IS [22].

E. Social Theories of Risk

The hypothesis on which sociological theories are based is that risk transposes objective knowledge. In these theories' philosophy, [23] believes that risk is strongly influenced by values, rationality, power, and emotions. Social views of risk are elaborated in the context of different phenomena studied and rooted in specific socio-cultural environments. However, their principles are valid in all social contexts, including risk in the microfinance industry [23], [24]. Risks are closely linked to

social phenomena, the interpretation of which is subjective depending on the social entity in question. Danaan [23] indicates risks are, therefore, not merely abstract technical calculations. In the study of STR and uncertainty, [20] identified five theories of risk and uncertainty: the risk society, governmentality, systems theory, cultural theory, and advanced work theory.

III. HYPOTHESES DEVELOPMENT AND RESEARCH MODEL

Hypotheses of the study are presented in the following subsections.

A. IT Capabilities, Information System Security, and Operational Risk

According to [25], "organizational IT capabilities as complex bundles of IT-related resources, skills, and knowledge, exercised through business processes, that enable firms to coordinate activities and make use of the IT assets to provide desired results". Resources refer to stocks of all accessible production factors owned or controlled by the firm [26]. However, capabilities "refer to a firm's capacity to deploy resources using organizational processes." Prior studies have found a positive link between IT resources and IT capabilities within an organization [27]. In the same vein, we propose the following hypothesis:

- H1: There is a positive relationship between IT resources and IT capabilities.

Actual "information system can be severely affected by security incidents" can comprise system integrity, confidentiality, and availability [28]. IT capabilities have been found to reduce information system-related risks and firm operational risks. An organization with an information system well organized reduces some risks related to Information system functioning of data safety. IT capabilities enhance information security by reducing computational and operational risks. The more the information system's security is guaranteed, the less likely it is that an operational risk will occur. Hence, we hypothesize as follows:

- H2: There is a positive relationship between IT capabilities and IS security.
- H3: There is a negative relationship between IT capabilities and perceived operational risk.
- H4: There is a negative relationship between IS security and perceived operational risk.

B. Factors of Operational Risk within Computerized Institutions

While using the system within companies, human errors have always been committed [29]. These errors may lead to the shutdown of operations. Even though the system and internal process are ready digitalized, factors such as user selves, familiness, and the user's environment may increase the operational risk. We, therefore, theorize that:

- H5: There is a positive relationship between user selves and perceived operational risk.
- H6: There is a positive relationship between familiness and perceived operational risk.

- H7: There is a positive relationship between environmental context and perceived operational risk.

C. Operational Risk, Credit Risk, and Reputational Risk

Based on Basel II Capital Accord, operational risk is defined as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, and from external events" [30]. Generated by various types of events [31], operational risk positively influences credit risk and reputational risk. [1]. At the same time, credit risks positively impact reputational risk. Therefore, we suppose that:

- H8: There is a positive relationship between operational risk and credit risk
- H9: There is a positive relationship between operational risk and reputational risk.
- H10: There is a positive relationship between credit risk and reputational risk.

D. Behavioral Bias, Tolerance Risk, and Reputational Risk

Behavioral bias consists of finance, economics, and cognitive psychology while making financial decisions [32]. Risk tolerance is the willingness to take the risk [1]. The maximum amount of risk tolerance is willing to be accepted in the financial decision-making process [33]. According to [1], behavioral finance biases and depositors' risk tolerance levels influence reputational risk. It is wiser to predict the same in the context of the microfinance industry.

- H11: There is a positive relationship between behavioral bias and reputational risk.
- H12: There is a positive relationship between tolerance risk and reputational risk.

E. Perceived Risk and Performance

Perceived risk refers to the expectation of loss [34], [35]. It is "a combination of uncertainty and the seriousness of outcome involved" [36]. The probability of loss may come from operational activities, credit-granting processes, and follow-up or reputational damage claims in the microfinance industry. Perceived risk being a negative valence can negatively affect the company's performance [6]. We then theorize that:

- H13: There is a negative relationship between operational risk and performance.
- H14: There is a negative relationship between credit risk and performance.
- H15: There is a positive relationship between reputational risk and performance.

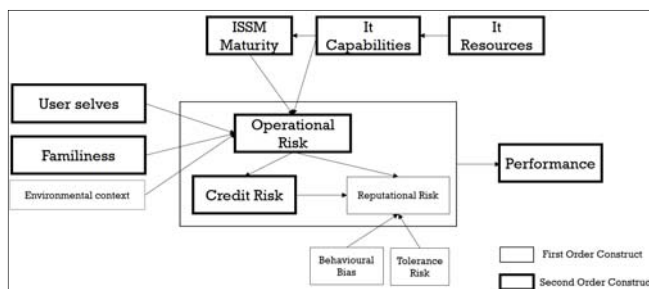


Fig. 1 Research model

IV. METHODOLOGY

To test the proposed model for this research, we plan to use a hybrid approach [37]. Mixed methods research is an approach in which the researcher gathers and draws conclusions using a combination of quantitative and qualitative research approaches [38], [39]. The primary purpose of applying both methods in the same study is to ensure complementarity, development, and expansion of the results [37], [40]. Indeed, studies in the literature such as [37] and [41] confirm that combining a single analysis quantitative and qualitative approaches allows for richer information and a better understanding of a phenomenon under study. A questionnaire erected from the literature will be used for quantitative data collection. After general data collection, primary data are obtained. These data will be quantitatively assessed according to the PLS-SEM method. Additionally, interviews will be conducted to strengthen and deepen quantitative findings.

V. EXPECTED CONTRIBUTION

This research will integrate information system risks, often overlooked, in the microfinance risk management system to enhance performance. Indeed, literature in operational risk management postulates that information technology and all resources capabilities reduce organizations' operational risks. Unfortunately, once adopted, new types of risks related to this digitalization emerge. These risks are often overlooked, yet their service is severe. Generally grouped into three main categories: risks affecting the organization of information systems, risks affecting the operation of information systems, and data security risks, the IT risk must be well managed to guarantee performance. Thus, this study proposes analyzing operational risk and offering mechanisms to reduce it within microfinance institutions, emphasizing the information system risk.

REFERENCES

- [1] Ferreira, S. J., E. Redda, and S. H. Dunga, *A structural equation model of reputational risk in South Africa*. Cogent Economics & Finance, 2019. 7(1): p. 1625739.
- [2] Zhong, X. and S. Zhou, *Risk analysis method of bank microfinance based on multiple genetic artificial neural networks*. Neural Computing and Applications, 2020. 32(10): p. 5367-5377.
- [3] Afolabi, T. S., T. M. Obamuyi, and T. Egbetunde, *Credit Risk and Financial Performance: Evidence from Microfinance Banks in Nigeria*. IOSR Journal of Economics and Finance, 2020. 11(1): p. 8-15.
- [4] Coetzee, J., *Bank Management in South Africa: A Risk-based Perspective*. 2016: Juta.
- [5] Kartalia, J., *Reputation at risk? Risk management*, 2000. 47(7): p. 51.
- [6] Cheng, L., et al., *Credit risk, operational risk, liquidity risk on profitability. A study on South Africa commercial banks. A PLS-SEM Analysis*. Revista Argentina de Clínica Psicológica, 2020. 29(5): p. 5.
- [7] Congo, B. C. D., *Rapport d'activités de la microfinance 2016*. 2016, Banque Centrale du Congo: Kinshasa.
- [8] Fadun, O. S. and D. Oye, *Impacts of Operational Risk Management on Financial Performance: A Case of Commercial Banks in Nigeria*. International Journal of Finance & Banking Studies, 2020. 9(1): p. 22-35.
- [9] Masakona, M., *The impact of digitisation on risk management in financial institutions*. 2019.
- [10] Meno, T., *An Assessment of Risk Associated with Digitalisation in the South African Construction Industry*. 2020: University of Johannesburg (South Africa).
- [11] Marc Andries; David Carteau, S. C. and P. G. C. G. C. L. Maguer, *Le*

- risque informatique, B.d.F. CPR, Editor. 2018.
- [12] Kozlenkova, I. V., S. A. Samaha, and R. W. Palmatier, *Resource-based theory in marketing*. Journal of the Academy of Marketing Science, 2014. 42(1): p. 1-21.
- [13] Wuen, C. H., F. Ibrahim, and K. J. Ringim, *The Impact of Human Resource Management Practices on SMEs Performance: An Exploratory Study in Brunei Darussalam*. International Journal of Asian Business and Information Management (IJABIM), 2020. 11(2): p. 68-87.
- [14] Teece, D. J., G. Pisano, and A. Shuen, *Dynamic capabilities and strategic management*. Strategic management journal, 1997. 18(7): p. 509-533.
- [15] Wang, C. L. and P. K. Ahmed, *Dynamic capabilities: A review and research agenda*. International journal of management reviews, 2007. 9(1): p. 31-51.
- [16] Nelson, R. R., *An evolutionary theory of economic change*. 2009: Harvard University Press.
- [17] Eisenhardt, K. M., *Agency theory: An assessment and review*. Academy of management review, 1989. 14(1): p. 57-74.
- [18] Wilson, R., *The theory of syndicates*. Econometrica: journal of the Econometric Society, 1968: p. 119-132.
- [19] Tate, W. L., et al., *An agency theory perspective on the purchase of marketing services*. Industrial Marketing Management, 2010. 39(5): p. 806-819.
- [20] Abdullah, H. and B. Valentine, *Fundamental and ethics theories of corporate governance*. Middle Eastern Finance and Economics, 2009. 4(4): p. 88-96.
- [21] Murengezi, C., *Impacts du crédit dans la promotion des PME: Études de cas sur la ville de Ouagadougou-Burkina Faso*. 2008: Presses univ. de Louvain.
- [22] Mayer, N., P. Heymans, and R. Matulevicius, *Design of a Modelling Language for Information System Security Risk Management*. 2007
- [23] Danaan, V., *Risk management in microfinance: identities, perceptions, behaviours and interests of microfinance stakeholders in Plateau State, Nigeria*. 2019.
- [24] Brown, P., *Risk and Social Theory: the legitimacy of risks and risk as a tool of legitimation*. 2014, Taylor & Francis.
- [25] Stoel, M. D. and W. A. Muhanna, *IT capabilities and firm performance: A contingency analysis of the role of industry and IT capability type*. Information & Management, 2009. 46(3): p. 181-189.
- [26] Amit, R. and P. J. H. Schoemaker, *Strategic assets and organizational rent*. Strategic management journal, 1993. 14(1): p. 33-46.
- [27] Ravichandran, T., C. Lertwongsatien, and C. Lertwongsatien, *Effect of information systems resources and capabilities on firm performance: A resource-based perspective*. Journal of management information systems, 2005. 21(4): p. 237-276.
- [28] Carmen, R. and P. Laura, *Operational Risk & Cybersecurity*. Management Strategies Journal, 2016. 32(2): p. 30-33.
- [29] Dávila-Aragón, G., H. X. Ramírez-Pérez, and S. Rivas-Aceves, *Familiness as determinant of operational risk: a bayesian analysis*. 2020.
- [30] Basel II, B. C. o. B. S., *Working paper on the regulatory treatment of the operational risk*, September, 2001.
- [31] Trenca, I. and I. Neag, *Considerations Regarding Operational Risk Management in the Context of the Basel II Agreement*. Romanian Economic Journal, 2010. 13(36): p. 171-185.
- [32] Zindel, M. L., T. Zindel, and M. G. Quirino, *Cognitive bias and their implications on the financial market*. International Journal of Engineering and Technology, 2014. 14(3): p. 11-17.
- [33] Grable, J. E., *Financial risk tolerance and additional factors that affect risk taking in everyday money matters*. Journal of business and psychology, 2000. 14(4): p. 625-630.
- [34] Crespo, A. H., I. R. Del Bosque, and M. M. G. de los Salmones Sánchez, *The influence of perceived risk on Internet shopping behavior: a multidimensional perspective*. Journal of Risk Research, 2009. 12(2): p. 259-277.
- [35] Sweeney, J. C., G. N. Soutar, and L. W. Johnson, *The role of perceived risk in the quality-value relationship: A study in a retail environment*. Journal of retailing, 1999. 75(1): p. 77-105.
- [36] Featherman, M. S. and P. A. Pavlou, *Predicting e-services adoption: a perceived risk facets perspective*. International journal of human-computer studies, 2003. 59(4): p. 451-474.
- [37] Kankam, P. K., *Approaches in Information Research*. New Review of Academic Librarianship, 2020. 26(1): p. 165-183.
- [38] Bryman, A., *Social research methods*. 2016: Oxford university press.
- [39] Santos, J. L. G. d., et al., *Mixed methods research in latin america: initiatives and opportunities for expansion*. Texto & Contexto-Enfermagem, 2020. 29.
- [40] Andrew, S. and E. Halcomb, *Mixed methods research for nursing and the health sciences*. 2009: Wiley Online Library.
- [41] Condomines, B. and É. Hennequin, *Studying sensitive issues: The contributions of a mixed approach*. RIMHE: Revue Interdisciplinaire Management, Homme Entreprise, 2014(5): p. 3-19.