DIGITALES ARCHIV

ZBW – Leibniz-Informationszentrum Wirtschaft
ZBW – Leibniz Information Centre for Economics

Bîlcan, Florentina Raluca; Ghibanu, Ionuț Adrian; Bratu, Ion Ionuț et al.

Article

Convergence and divergence regarding the impact of risks on banking transactions

Academic journal of economic studies

Provided in Cooperation with:
Dimitrie Cantemir Christian University, Bucharest

Reference: Bîlcan, Florentina Raluca/Ghibanu, Ionuț Adrian et. al. (2019). Convergence and divergence regarding the impact of risks on banking transactions. In: Academic journal of economic studies 5 (4), S. 145 - 150.

This Version is available at:
http://hdl.handle.net/11159/4128

Kontakt/Contact
ZBW – Leibniz-Informationszentrum Wirtschaft/Leibniz Information Centre for Economics
Düsternbrooker Weg 120
24105 Kiel (Germany)
E-Mail: *rights[at]zbw.eu*
https://www.zbw.eu/econis-archiv/

Standard-Nutzungsbedingungen:
Dieses Dokument darf zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden. Sie dürfen dieses Dokument nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen. Sofern für das Dokument eine Open-Content-Lizenz verwendet wurde, so gelten abweichend von diesen Nutzungsbedingungen die in der Lizenz gewährten Nutzungsrechte.

https://zbw.eu/econis-archiv/termsofuse

Terms of use:
This document may be saved and copied for your personal and scholarly purposes. You are not to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public. If the document is made available under a Creative Commons Licence you may exercise further usage rights as specified in the licence.

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Mitglied der Leibniz-Gemeinschaft

Academic Journal of Economic Studies
Vol. 5, No. 4, December 2019, pp. 145–150
ISSN 2393-4913, ISSN On-line 2457-5836

Convergence and Divergence Regarding the Impact of Risks on Banking Transactions

Florentina Raluca Bîlcan[1], Ionuț Adrian Ghibanu [2], Ion Ionuț Bratu [3], George Adrian Bîlcan[4]

[1,2,3,4] Valahia University, [1]E-mail: bilcan.florentina.raluca@gmail.com, [2]E-mail: ghibanu.ionut.adrian@gmail.com,
[3]E-mail: bratu.ion.ionut@gmail.com, [4]E-mail: bilcan.george.adrian@gmail.com

Abstract

Risk is a permanent companion to banking transactions, which is why the cyber strategy will be affected if current and future risks are not taken into account. In order to identify and evaluate the risks of information security, any economic entity must start from its main lines of activity, from the strategy it will adopt. The paper presents not only the traditional aspects of information security risks in banking transactions, but also the way in which risk management becomes especially important in overcoming less predictable cyber attacks. The results show that identifying, analyzing and managing the security risks of information specific to banking transactions, several important pieces of the puzzles are represented by the models and techniques that address these risks.

Keywords

Banking transactions, risk, probability, cyber attacks

JEL Codes: D80, D81

© 2019 Published by Dimitrie Cantemir Christian University/Universitara Publishing House.

(This is an open access article under the CC BY-NC license http://creativecommons.org/licenses/by-nc-nd/4.0/)

Received: 07 November 2019 **Revised: 28 November 2019** **Accepted: 12 December 2019**

1. Introduction and literature review

In the first stage of global risk management and monitoring, the risks associated with each type of transaction must be determined (Singh and Fhom, 2017). Some risks of information security are obvious, others cannot be identified, regardless of the working procedures and techniques used, in order to prevent them, until the triggering and causing of losses in the respective transactions (Core, 2015; Heffernan, 2005; Peltier, 2010).

In the opinion of many authors, any banking transaction involves a procedure and therefore the detection and anticipation of new accidental risks, having a very important role in the financial planning process (Lu and Chen, 2011; Banks and Dunn, 2003; Shaikh *et al.*, 2017). Once the security risks of the identified information have been identified, the main types of control activities must be determined for each type of risk, knowing the characteristics and their probable evolution. The adverse action of a risk factor can be diminished and/or in some cases avoided, by knowing and removing the cause that causes it (Winkler, 2010).

The term bank risk refers to those risks that banks face in their current operations and not just the risks associated with the traditional banking activity. Bank risk is generated by a large number of operations and procedures. Bank risks should be inventoried and defined as best as possible in the perspective of analyzing their measurement and control (Van Greuning and Brajovic, 2003).

The specialized literature (Bessis, 2005; Duffie and Singleton, 2003; Stepchenko and Voronova, 2015) also includes bank risk classifications, depending on: risk exposure, risk genesis, nature of risks, risk allocation in transactions. The analysis of banking risks is usually addressed by types of risks, due to their complexity and diversity. However, we must bear in mind that the bank's exposure is made for all the risks and that, moreover, the risks are interdependent. This reality requires a global approach to risk management, which must provide the bank with the ability to identify and assess risks, to control them, to eliminate or avoid them and to finance them (King and He, 2006).

It should be emphasized that the imperfections of the capital market, such as taxes and bankruptcy costs, give a significant importance to risk management (Al Sukkar and Hasan, 2005). Thus, the lack of resources can be an explanation for this situation, especially due to the fact that the training of personnel for acquiring the necessary skills for trading derivative financial products requires significant investments.

In order to reduce the risks, methods can be used such as: redesigning the associated activities and the flows of operations; the elimination of products considered risky or whose operational procedures are little known (e.g. derivatives). The risk transfer is more appropriate in the event of the occurrence and action of very serious, unpredictable events, the operation of the method assuming the existence of conventional insurance markets (Lu *et al.*, 2005).

From the existing literature at the national level, we must mention a series of studies that argue the need to adapt the banking transactions regarding the risk management in order to align us with the existing requirements at the international banking system. It also underlines the need to carry out this process at the fastest possible (Collins and McCombie, 2012; Singh and Fhom, 2017).

Risk management in banking transactions first addresses the quantifiable risks (Core, 2015). This is especially the case of the financial risks that arise on the financial markets and which result in unfavorable evolutions of the financial statements or the results of the institution, as a result of the unpredictable changes registered in the financial markets (Winkler, 2010).

In this context, it appears necessary to review the international regulations in the field of banking risk by continuously adapting the risk management methods to the economic realities in order to be able to identify early on the existence of disruptive factors. Banks can only successfully manage banking risks if they recognize the strategic role of managing information security risks, if they use analysis and management to increase efficiency, if they take precise risk-adaptation measures (Natarajan *et al.*, 2010).

Throughout this article, theoretical and practical aspects are met, quantitative and qualitative analyzes, all aimed at identifying, analyzing and controlling the risks of information security and not least, managing the risk in banking transactions.

2. Convergence and divergence regarding the impact of risks on banking transactions

In the banking universe, risks are multiple and multidimensional and interdependent, which is why they need to be listed and defined as best as possible in terms of their measurement, monitoring and control. Over the past several years, reducing or avoiding risks requires prior identification and quantification of risks.

According with Bessis (2005) the risks can be covered by the following techniques:

- elaboration of a formal financing program based on the forecasts regarding the anticipated losses;
- withdrawal of reserve funds for credit losses;
- passing the losses on expenses or covering them from the capital, to the extent that these losses occur;
- establishing risk provisions.

Beyond the uncertainty associated with the expenses it generates, managing information security risks can be a positive message for financial markets (Heffernan, 2005). The risk coverage must be based on two criteria:

- coverage of risk families;
- the existence of own statistical databases regarding the frequency and extent of the risks.

Assuming the global information security risk generates the obligation of the banking company to comply with the so-called banking prudence rules (King and He, 2006). On the other hand, the purpose of the risk management activity is to optimize the risk-profit ratio, which is a determining factor of the banking strategy. Risk management gives the bank management a better vision of its future and its ability to be competitive in the market. Ignoring present and future risks can lead to serious future losses and even bank failure (Peltier, 2010).

According to specialized studies, risk knowledge is useful and necessary information in establishing the appropriate fees and bank charges (Agrawal and Tapaswi, 2017; Joseph *et al.*, 2010). The estimated risks as costs will be included in the price of the services offered to the customers when the market allows it. The performance measurement involves the analysis of qualitative and quantitative indicators, aimed first and foremost at determining the bank's soundness, its degree of risk exposure and then its efficiency level.

The role of bank management in managing the security risks of information is a protective filter (Arukonda and Sinha, 2015), the objectives being:

- maximizing bank profitability;
- minimizing risk exposure;
- compliance with the quality and prudential norms.

The risk indicators gain more relevance in a general context of appreciation of the bank's profitability and its market competitiveness, the final objective of bank management consisting, in addition, in maximizing the income of the adjusted shareholders (Duffie and Singleton, 2003). The level of risks generated by a bank is influenced by controllable and

uncontrollable factors. Banks cannot control these external factors but they can formulate flexible plans to react to these factors (Lu and Chen, 2011).

Given the transposition of the classic functions of general management to the problem of information security risk (Malatras *et al.*, 2016), removing this risk becomes a decision problem, which can take the following forms:

- routine decisions consisting of the application of known measures, the effectiveness of which has been verified;
- adaptive decisions that consist in adapting the parameters of the decision to a situation that knows changes to the reference situation;
- innovative decisions that involve making new decisions.

The evaluation of the information security risk management policy consists of measuring the performances obtained as a result of the exposure to the risk and offers the possibility of optimizing the future policies based on the weaknesses and strengths identified (Al Sukkar and Hasan, 2005).

Some authors believe that banks are pursuing objectives that are often divergent, in the sense that they use specific tools both to increase their market share and to attract available capital needed to carry out speculative transactions (Milunovich and Yang, 2018; Collins and McCombie, 2012; Van Greuning and Brajovic, 2003). Other authors consider that in order to prevent systemic risk, in order to ensure the stability and viability of the entire banking system, the monetary authorities have developed systems to monitor the activity of banks and the transactions carried out within banks (He *et al.*, 2012; Winkler, 2010). All banking systems have at least one regulatory and supervisory authority, which have different responsibilities, powers of regulation and implementation of assumed decisions.

In the American approach to the risk position of a bank, comprehensive models of risk assessment of banking transactions involve an assessment of the risk of information security of the bank by quantifying all the risks corresponding to each separately treated transaction and assigning certain scores for each transaction (Natarajan *et al.*, 2010). The scores are then aggregated to obtain the final score of the bank as a whole.

It should also be noted that statistical models have the advantage that they identify those risks that are most likely to generate adverse situations for the bank, based on the forecast of the probability of future developments (Kurosawa *et al.*, 2017). These models remove all the disadvantages of using static models in an economy characterized by dynamism.

Supervisors, as well as theorists, are paying close attention to macro-prudential analysis to assess the vulnerability to cyber-attacks of banking systems (Fischbacher-Smith, 2016). The novelty of this recent approach, established in the late 1990s, is that the systemic risk is analyzed from the perspective of its interaction with current challenges regarding the security risk of information in the digital economy, the focus of the supervisory activity being on the exposure cyber attacks (Broadbent and Schaffner, 2016). We therefore assist in minimizing the specific factors of each bank that may have an adverse evolution and may increase the risk exposure.

The second aspect concerns the perspective of how sustainable is cyber security risk assessment and measurement (Arukonda and Sinha, 2015). The information security risk measurement system used by a bank must identify all the sources that generate this type of risk and must be able to evaluate the effects of a cyber attack.

The risk analysis goes through the study of the functional needs of the security and through the determination - depending on the foreseeable consequences of a disaster - of the properties to be insured. Risk assessment involves qualitative and quantitative factors (Bessis, 2005).

Risk assessment is therefore very difficult and totally dependent on a specific environment (Peltier, 2010). The evaluation phase will allow you to define a target for functional security (regardless of tools or tools). Finally, the analysis of the means (the audit of the instruments and inventories) and the choice of the means will allow the application of preventive security measures taking into account the value-threat couple.

While access control is essentially based on the verification of the identity of a logical entity, material or human, the notion of multilevel security associates different levels of access control, to best protect a resource, regardless of its nature. The reverse of this medal is that such a security structure has no friendliness and/or leads to degradation of the system's performance.

The position occupied today by technologies in security management is likely to vary quite strongly depending on the applications concerned (Milunovich and Yang, 2018). In addition, it should not be assumed a priori that a successful recipe in one place will do the same wonders in another. The mission of the systems is therefore to see and prove.

In the current period, marked by the increasing complexity and diversification of the types of transactions that take place on the foreign exchange market, the risk generated by international transactions is associated with the potential gains or losses in a transaction that is sensitive to the exchange rate change (Kurosawa *et al.*, 2017). As banks are heavily anchored in international financial operations, the degree of exposure to information security risk increases. However, due to the varied typology of information security risk and the possibility of exposure to concomitant risks, information security risk management aims at managing the risk of trading and managing traditional banking operations.

If the bank conducts foreign exchange trading activities, proper management imposes certain limits on the view positions for each currency, including the size of non-correlations in the case of transactions with derivative financial products. Therefore, a limitation of the maximum value of a transaction expressed in foreign currency or of all assumed transactions significantly reduces the information security risk.

3. Results and discussions

In banking, risk should be regarded as a conglomerate or complex of risks, often interdependent, having common causes or producing a type of risk generating a chain of other risks (Shaikh *et al.*, 2017).

The reality highlights that the bank, in its activity, is subject to risks on two levels:

- on the one hand, the bank is an organization and is liable to face the risks inherent to any entity;
- on the other hand, the bank functions as a specific intermediary in the process of capital circulation and engages in the classic banking risks related to the partnership (counterparty risk).

The management of the risks facing the banking activity can be ensured not only by such an efficient computer system, but especially by the human factor, its intervention being particularly important in analyzing the data provided by the system and taking decision.

Establishing the information that will be provided by the system is one of the main tasks of the analysts who design it and the experts who use it. Therefore, the quality of the decision-making act depends both on the informational value provided in the reports generated by the system, and on the capacity of analysis and experience of the specialists of the institution using the system.

The tools of analysis and assessment are aligned with those used in other spheres, but the specifics print them as one will see their own individuality. For example, interactive financial forecasting models operate in a manner close to that of spreadsheets, being characterized by:

- are stronger, being the most complex computer models of forecasting;
- can be used on personal computers with strong memory or on industrial computers;
- allow to find a certain variable that will produce a certain desired effect;
- can be networked, allowing more users to use the data and the program;
- allow the user to specify the variables in the form of distribution probabilities and not as discrete values;
- simulates real-world situations, randomly selecting a value from each likely distribution range and then calculating a set of results associated with the chosen value;
- the probabilities used can be estimated using databases containing information from previous periods.

The choice of the strategy that will be used in the simulation can be based both on the analysis of the input data (historical data in evolution and the previous objectives proposed), as well as on the experience gained in performing similar simulations.

Multifactorial models have opened a new perspective in addressing the risk associated with financial investments, by including in the analysis of a complex of factors that explain with greater accuracy the systematic risk. Because portfolio diversification makes non-systematic risk negligible, it means that the systematic risk associated with the single factor (the market) is the only one that gives the size of the risk premium associated with the investments in the financial markets and which directly influences the size of the expected gain.

At the same time, the objective of risk management is to minimize it, so that it is possible to maximize the value of the bank. Some economists consider that banking risk management is a part of financial management, along with financial planning and forecasting, accounting systems, internal controls and treasury (Collins and McCombie, 2012; Duffie and Singleton,

2003; King and He, 2006). This approach turns out to be from a narrow perspective; in fact risk management has to respond to a number of challenges.

Quantifying information security risks involves using the techniques, tools and skills necessary for the bank to offset these risks. The development of quantitative modeling tools allows performing simulations that are useful in analyzing the effects induced by the rapid changes occurring in the banking environment, as well as their impact on transactions. The existence of some bank risk management techniques presents important advantages for the banking institution, and their lack can have serious consequences. Thus, risk management should be the number one priority of all those involved in the bank's management activity.

4. Conclusions

The current period is called the era of information security risk management in banking, and the analysis and management of this risk is an extremely complex and important task of banking management. In order for the security risks of the information to be rigorously managed and monitored, it must first of all be identified, known and applied tools and techniques to diminish or avoid their influence on the banking activity.

Under the current conditions of the Romanian banking system, the evolution and weight of the expenses regarding reducing the security risks of the information are very different from one bank to another. And in the future, the expenses related to the development, expansion and improvement of the computer network, implementation of some products and, in particular, new services will continue to increase in total expenses, having as a natural effect the development and consolidation of each bank.

We believe that proper risk management should provide the bank with the ability to identify, quantify and monitor the risk profile, as well as to avoid and finance them. These elements are in fact found in the management of each type of risk, but at the global level it acquires a new dimension. The success of managing information security risk also depends on the bank's ability to anticipate potential attacks, the transfer of losses, as well as the degree of their integration into the bank's overall management system. In addition, volatility of the financial market emphasizes the need to analyze and manage the risks of information security, all the more so as the phenomenon becomes increasingly powerful in the Romanian economy, with profound meanings for the present, but especially for the future.

Acknowledgement

This work is supported by project POCU 125040, entitled "Development of the tertiary university education to support the economic growth - PROGRESSIO", co-financed by the European Social Fund under the Human Capital Operational Program 2014-2020

References

Agrawal, N., & Tapaswi, S. (2017). Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey. Journal Information Security Journal: A Global Perspective, 26(1), 1-13.
Al Sukkar, A., & Hasan, H. (2005). Toward a model for the acceptance of internet banking in developing countries. Information Technology for Development, 11(4), 381-398.
Arukonda, S., & Sinha, S. (2015). The innocent perpetrators: reflectors and reflection attacks. Advanced Computer Science, 4, 94–98.
Banks, E., & Dunn, R. (2003). Practical risk management. An executive risk to avoiding surprises and losses., John Wiley & Sons, Ltd, Chichester.
Bessis, J. (2005). Risk Management in Banking, John Wiley & Sons, Ltd., Chichester.
Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78(1), 351- 382.
Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. Journal of Policing, Intelligence and Counter Terrorism, 7(1), 80-91.
Core, F (2015). Big data analytics: a managerial perspective, Springer.
Crouhy, D., & Robert M. (2006). The Essentials of Risk Management, Editura McGraw Hill Companies.
Duffie, D., & Singleton, K. J. (2003). Credit Risk, Pricing, Measurement and Management, Princeton University Press
Fischbacher-Smith, D. (2016). Breaking bad? In search of a (softer) systems view of security ergonomics. Security Journal, 29(1), 5-22.
He, D., Chen, C., Chan, S., & Bu, J. (2012). Secure and efficient handover authentication based on bilinear pairing functions. IEEE Transactions on Wireless Communications, 11(1), 48–53
Heffernan, S. (2005), Modern Banking, John Wiley & Sons Ltd, England.

Joseph F. Hair, J., Black, W. C., Babin, B. J., & Anderson, P. E. (2010). Multivariate Data Analysis (Seventhed.). New Jersey: Pearson Prentice Hall.

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. Information and Management, 43(6), 740-755.

Kurosawa, K., Ohta, H., & Kakuta, K. (2017). How to make a linear network code (strongly) secure? Designs, Codes and Cryptography, 82(3), 559- 582.

Lu, H. P., Hsu, C. L., & Hsu, H. Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. Information Management and Computer Security, 13(2), 106-120.

Lu, Y.R., & Chen, Z.J. (2011). Revised KMV Model to Our Listed Companies Analysis of Applicability of Credit Risk Measurement. Research of Finance and Education, 1, 68-73.

Malatras, A., Geneiatakis, D. & Vakalis, I. (2016). On the efficiency of user identification: a system-based approach. International Journal of Information Security, 15(1), 1-19.

Milunovich, G.& Yang, M. (2018). Simultaneous Equation Systems with Heteroscedasticity: Identification, Estimation, and Stock Price Elasticities. Journal of Business & Economic Statistics, 36, 288–308.

Natarajan, T., Balasubramanian, S., and Manickavasagam, S. (2010). Customers choice amongst self service technology (SST). Channels in retail banking: a study using analytical hierarchy process (AHP). Journal of Internet Banking and Commerce, 15(2), 35-45.

Peltier, T.R. (2010). Information security risk analysis, Third Edition, CRC Press, Taylor & Francis Group, Auerbach Publications.

Shaikh, A.A., Glavee-Geo, R., & Karjaluoto, H. (2017). Exploring the nexus between financial sector reforms and the emergence of digital banking culture–Evidences from a developing country. Research in International Business and Finance, 42, 1030-1039.

Singh, A. & Fhom, H.C.S. (2017). Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. International Journal of Information Security, 16(2), 195-201.

Stepchenko, D., & Voronova, I. (2015). Assessment of Risk Function Using Analytical Network Process. Inzinerine Ekonomika-Engineering Economics, 26(3), 264-271.

Van Greuning, H., & Brajovic, B. S. (2003). Analyzing and Managing Banking Risk. A Framework for Assessing Corporate Governance and Financial Risk, Second Edition, The World Bank, Washington, D.C.

Winkler, I. (2010). Justifying IT Security – Managing Risk & Keeping your network Secure, Qualys Inc.