

Article

Risks of Banking Services' Digitalization: The Practice of Diversification and Sustainable Development Goals

Francisco Zabala Aguayo ¹ and Beata Ślusarczyk ^{2,3,*} 

¹ Economic Analysis and Political Economy Department, Universidad de Sevilla, 41018 Seville, Spain; fزابالا@us.es

² Faculty of Economic and Management Sciences, North-West University, Vaal Triangle Campus, Vanderbijlpark 1900, South Africa

³ The Management Faculty, Czestochowa University of Technology, 42-201 Czestochowa, Poland

* Correspondence: beata.slusarczyk@wz.pcz.pl

Received: 1 April 2020; Accepted: 11 May 2020; Published: 14 May 2020



Abstract: The study aims to investigate threats that might occur in diversification management, operational risks of banking services in the process of digitalization, as well as the impact on customers and banks. The right choice of a risk management model for a bank plays an important role in the sustainable development of competitiveness and the transformation of banking activities in the future. This work assesses bank risks and determines information risks in relation to the total capital of Santander Bank of Spain. The authors adapted an operational risk management (ORM) model to minimize the risks of the bank's digitalization and upcoming operational risks. The ratio of the total operational risk to the total bank's capital was 0.65%, which is below the permissible minimum value and is acceptable. Based on this indicator, diversification of business risks can be applied. As a result of the study, the total value of operational risks was calculated and the acceptability of this indicator to the capital of Santander Bank was assessed, which allowed the authors to assess whether the value was critical. In addition, it was also revealed that the main external risk of Santander Bank in 2018 was fraud in the use of online payments. The results might help to more effectively evaluate insurance payments for identified operational risks and effectively make decisions and optimize reporting documents of banks.

Keywords: sustainable development; global banking ecosystem; sustainable financing; cyberattacks; digitalization; diversification risk; operational risk

1. Introduction

The digitalization of decision-making processes and various operations helps to maintain a customer base and increase banking business using new electronic channels and online lending. In general, this contributes to an increase in the efficiency and competitiveness of banks, as well as a decrease in the time for customer service [1]. Creating platforms for banks increases their attractiveness for customers and stakeholders of an interconnected business, thereby providing opportunities for creating an ecosystem of banks [2]. Social factors and the development of new digital information technologies have a positive effect on investments in banks [3,4].

The prospect of creating new services for small businesses, such as online accounting, operational accounting, taxation, profit forecasting, and the creation of ecosystems, makes it possible to take into account the needs of customers in the future. However, digitization of data creates about 70% of digital risk for banks. According to the analysis, 22% of banks around the world have invested more than 25% of their annual budget to digitize risk management [5]. An improved regulatory framework will allow

faster digitization of banking services [6]. Diversification of bank risks is one of the main methods for the sustainable development of banks in the global economy. In this situation, risk diversification management requires a new strategy in the context of digitalization. Diversification of the risks of the loan portfolio allows one to increase profits and reduce the overall risks of banks.

An analysis of the impact of various diversification strategies of operational risks in developing countries (Philippines, Vietnam, Malaysia, Indonesia, Thailand) shows that banks have become more competitive and financial institutions have become more sustainable [7]. In the banks of Indonesia and Thailand, diversification most positively affects banks' work and risk management. In the Philippines, asset diversification has a positive effect on efficiency, but does not affect profitability. In Malaysia, the diversification of assets negatively affects profit, but increases efficiency and positively affects risk management [8]. In Vietnam, diversification has no practical effect on bank performance due to an underdeveloped market [9]. Asian banks do not diversify lending activities to increase profits in the context of liberalization. Asian banks diversify interest-free assets and services that are not related to lending in order to increase profits [10]. The Asian experience is useful for developing countries in terms of gaining additional knowledge about the impact of risk diversification of the banking system, because these countries have liberalized their financial sectors [11]. Diversification of the investment portfolio in the stock market can be used to increase portfolio returns and reduce the risk of lower share prices. Therefore, income from activities in the stock market is the reason for diversification in order to increase the efficiency of banks and reduce risks.

Diversification of bank risks and activity helps attract investment [12–16] and reduces the impact on interconnected markets [17]. Previous studies of Chinese banks have shown that geographic diversification of banks increases market share, net margin, and non-interest income, as well as increasing operating costs through expansion [18].

In the modern world, insufficient attention is paid to research related to the impact of digitalization on the effective operation of the banking system and the cooperation of FinTech companies with banks [19]. Providing complete cybersecurity for mobile banking creates the prerequisites for online fraud, which could make smartphones less reliable in the future [20]. The goal for the development of bank cybersecurity is the creation of a mechanism for protecting information in the banking sector [21,22]. Most small commercial banks do not have sufficient resources for cybersecurity [23]. The main problem in the area of cyberattack risks for banking institutions is certain regulatory and supervisory requirements to regulate such risks [24]. There is a need for changes in regulatory documents in order to develop the banking sector and effective risk management [25]. The mobile payment ecosystem, with which each client can independently control his/her own information, has not been practically clarified in previous studies [26].

To facilitate access to a large amount of online information 24 h a day, further studies of the cost and logistics of providing electronic banking services are required [27]. Round-the-clock banking services will reduce staff costs and increase access to banking services. Particular attention in Europe is paid to the digitalization of online bank accounting [28].

The introduction of common payment standards in the Eurozone and the creation of a single pan-European payment area—the Single Euro Payments Area (SEPA)—facilitate the provision of banking services throughout the European Union. The introduction of the Payment Services Directive PSD2, the entry of Google and Apple into the payment services market, and the continuous growth of the FinTech industry are forcing banks and other financial institutions to strengthen the integration of operations with innovations. It is extremely important for existing banks to implement flexible working methods to meet constantly changing and growing customer expectations, as a result of which so-called “electronic banking” has appeared, which represents a multifunctional system of informing the client and remote management of his/her accounts [29]. Electronic banking services include:

1. account statements for a customer;
2. information on banking products (deposits, loans, securities);
3. applications for opening deposits and obtaining loans and bank cards;

4. internal transfers to bank accounts;
5. transfers to accounts in other banks;
6. currency conversion [30].

If the first two types of services can be carried out using only mobile communications, the rest, as a rule, require an internet connection.

In 2007, 25% of the adult population of the EU countries used e-banking services, in 2011 this indicator grew to 40%, and in 2018 it reached 48%. Among internet users, the share of users of electronic banking services grew from 44% in 2007 to 54% in 2011, and to 59% in 2018 [31]. If in the whole EU the share of the population that used electronic banking services was equal to 46% in 2018, then in 15 countries it was higher than the average. These countries were Norway—90%; Finland—86%; Netherlands—85%; Denmark—85%; Estonia—81%; Sweden—80%; Luxembourg—65%; Latvia—64%; Belgium—62%; France—58%; Austria—51%; Lithuania—50%; Czech Republic—48%; Malta—47%. However, in a significant number of European countries, the indicators of the use of electronic banking services were below the average level: Spain—39%; Hungary—34%; Slovenia—34%; Croatia—33%; Poland—31%; Portugal—28%; Italy—28%; Cyprus—20%; Greece—14%, Bulgaria—7%, Romania—5%.

At the same time, in the past five years, Spanish banks have been more profitable than European Union banks. Making a profit in the banking sector is important for shareholders as well as for the accumulation of reserves, which distinguishes Spain from other countries. This has created an asymmetry in the volume of activity of Spanish banks and their willingness to provide digital account services, the demand for which is growing from year to year [32]. This determined the motivation and purpose of this study. The aim of this study is to identify operational risk in order to minimize the financial consequences of sustainable development for digitizing Spanish banks, as well as improve the method of managing banks in the context of digitization, using the example of Santander Bank.

This study is presented in five sections. The introduction presents the theoretical basis of the studied problems. The methods section describes the procedures and approaches that have been used to achieve the goal of the study. The results section includes the main analytical conclusions of the performed work. The discussion presents additional and alternative views on the processes of digitization of banking services and the risks arising in this context. The conclusion summarizes the work done, its implementation value, and indicates the vectors of further research.

2. Methodological Framework

The implementation of Basel II (that is, recommendations for managing operational risk) becomes a key factor that raises banks' reliability rating and arouses investor confidence and interest [33]. Therefore, the study used an optimized approach to measurements (AMA) under Basel II, which allowed the authors to simulate the operational risk of the study object (Santander Bank). The model includes indicators such as:

- threat of defects and failures;
- threat of loss of data integrity and unauthorized access to customer data;
- threat of violation of a technical system in an information space;
- threat of cyberattacks;
- level of annual defects;
- current annual loss from defects;
- current annual loss of data integrity and unauthorized access to customer data.

Operational risk management is based on identifying sources of operational risk, identifying operational risks, assessing operational risks, monitoring operational risks, and controlling and minimizing operational risks. The research design and its procedures were built on these elements. This was based on the assumption that the likelihood of events associated with operational risk increases when negative signals appear from indicators (key performance indicators, key control

indicators, key risk indicators) of each of the elements. Accordingly, the risk manager can prevent such danger by strengthening control over the situation, which is implemented through the integrated ORM model. Based on ORM practices for minimizing risks of a bank's digitalization, the authors optimized the method of managing sustainable development for digitalization of Santander Bank of Spain (Figure 1).

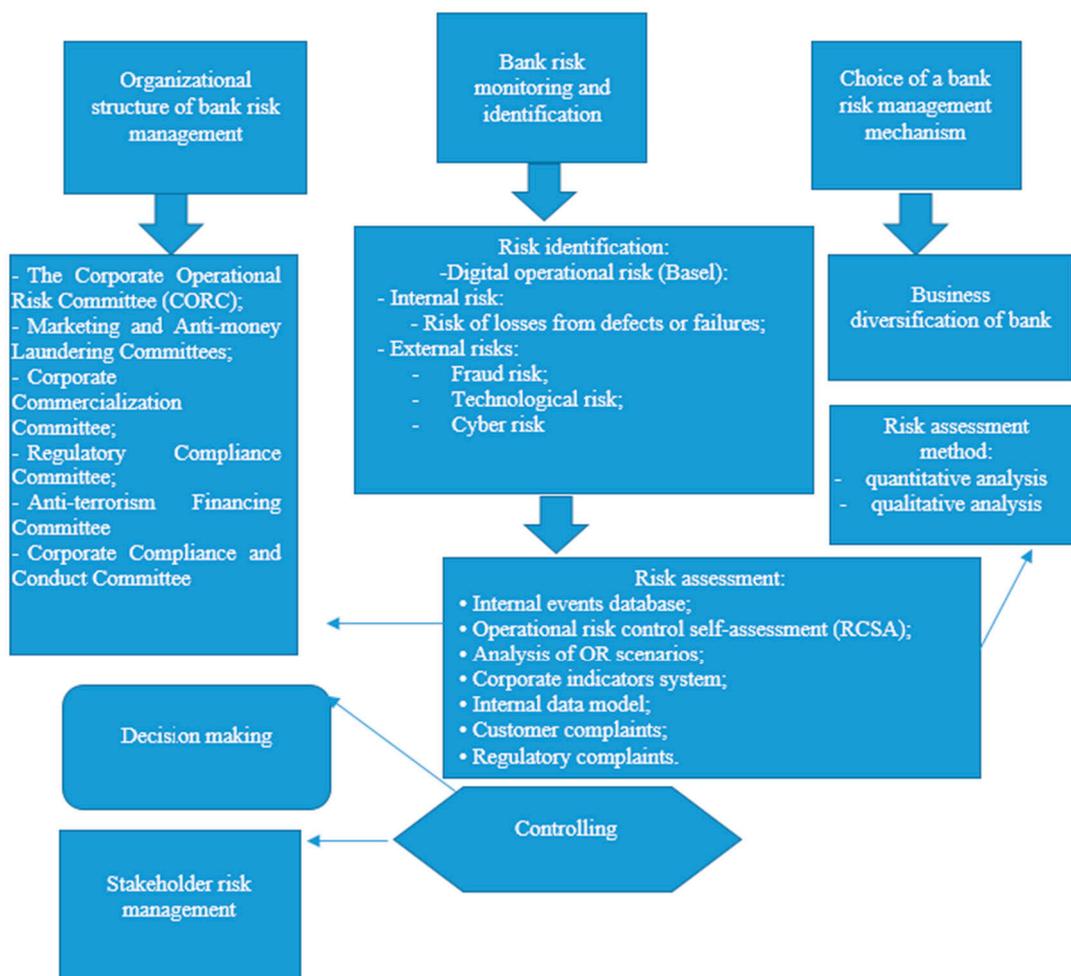


Figure 1. Method of managing digitalization risks in Santander Bank of Spain. Source: developed by the authors.

3. Results

Using an optimized approach to measurements (AMA), the authors applied the method of modeling the operational risk of Santander Bank (Spain) under Basel II and, in the context of the digitalization of Spanish banks at the first stage of monitoring and identification of risks, the authors identified the potential threats of risk [34].

Stage one—monitoring and risk identification:

1. The threat of defects and failures.
2. The threat of loss of data integrity and unauthorized access to customer data.
3. The threat of violation of the technical system in the information space.
4. The threat of cyberattacks.

Stage two—risk assessment:

We evaluated the risks according to the formula:

$$\text{Event onset} = (1 - \text{threat elimination}) * (1 - \text{threat identification}) * (1 - \text{threat level}), \quad (1)$$

The level of annual defects and failures was calculated by the formula:

$$\text{Annual loss rate (1-4)} = \text{Annual loss} * \text{Annual number of threats}, \quad (2)$$

where:

$$\text{annual number of threats} = \text{Event occurrence} * \text{Annual forecast of the number of threats}, \quad (3)$$

The current annual loss from defects and failures is calculated by the formula:

$$\text{Current annual loss (1)} = (\text{past annual loss} - 1) * \text{average growth}, \quad (4)$$

The current annual loss from loss of data integrity and unauthorized access to customer data was calculated by the formula:

$$\text{Current annual loss (2)} = (\text{past annual loss} - 1) * \text{average growth} * \text{the time of loss}, \quad (5)$$

The current annual loss from a violation of the technical system in the information space and cyberattacks was calculated by the formula:

$$\text{Current annual loss (3,4)} = \text{the time of loss} * \sum_{i=1}^8 \text{average hourly profit} * \text{loss coefficient of information failures}, \quad (6)$$

The data showed that the internal risk of losses from defects or failures was 84% and the external risk was 14% (Table 1).

Table 1. Assessment of information systems risks.

Operational Risks	1 Threat	2 Threat	3 Threat	4 Threat
Internal risks			36.0 million US dollars	
External risks	10.8 million US dollars	2.4 million US dollars		10.8 million US dollars
Total:			60.0 million US dollars	

Source: developed by the authors based on data from the Santander Consumer Bank, 2018–2019 [2,35,36].

To identify the adequacy of this method, it was necessary to correlate the estimated risks with capital according to the formula:

$$\text{Min}_{\text{est.risks}} = \frac{\sum \text{Orisk}}{\text{Capital}} * 100\%, \quad (7)$$

$$\text{Min}_{\text{est.risks}} = \frac{60 \text{ ml.dol.}}{9.3 \text{ bl.dol}} * 100\% = 0.65\%, \quad (8)$$

The minimum acceptable value of the total operational risk is 1%. Let us conclude that the estimated total minimum value of operational risk was 0.65%, accordingly below the permissible minimum value. Therefore, the total cost of threats (1–4) for operational risks was acceptable in relation to the capital of Santander Bank; threats need to be eliminated only if the value is critical. If the minimum value is not met by the set parameter, then the threats are adjusted from invalid values

to acceptable ones, and then the minimum operational risks are assessed again until the minimum acceptable risk value is met. The main external risk (fraud) in 2018 was traced to use of online payments.

The number of new cyberattacks in the world is growing. According to KPMG's Global Banking Fraud Survey, cyberattacks led the list of financial institution risks in 2019 [37]. Today, many researchers pay attention to the use of artificial intelligence for phishing attacks [38,39]. All this increases the risks of cyber threats to the banking system. Small banks remain the most vulnerable since they are not able to allocate large budgets for cybersecurity.

The main causes of cyber threats for a bank can be divided into several groups:

- lack of permanent updating of legislation and common safety standards;
- lack of funding from the banks themselves;
- lack of corporate culture in the field of cybersecurity within the bank.

All this requires the inclusion of the following elements in the operating activities of Santander Bank:

- training of cybersecurity personnel in the format anytime, anywhere (training materials should be submitted in a simplified way for perception: through animation, videos and other "convenient" tools. After each stage of training, formal and covert testing should be organized; for example, phishing emails can be sent to verify employees' reactions. It can also be effective to periodically send out reminders about information security requirements with information on the latest events and news, which will help staff to stay updated on the latest trends and perceive cybersecurity as a daily task);
- developing a plan in case of an attack (this plan describes the actions of various team members in different scenarios of the incident, from attacking a website to stealing money from customer accounts. Discussing an action plan with professional moderation will allow identifying key problems that need to be addressed before the bank system is hacked. It is also of relevance to create security operations centers that conduct cyber intelligence, monitor threats, and respond to them in a timely manner);
- regular conduct of cybersecurity audits (an important aspect is the qualification of the auditor: he/she must have sufficient competence to identify bottlenecks in bank security);
- training customers in basic security rules (this will help reduce the additional risks of unauthorized access to information through one-time passwords and two-factor authentication).

4. Discussion

The value of acceptable risk was achieved through the selected risk management mechanism of the bank—business risk diversification—in order to increase effective sustainability, which has been achieved through the development of global digitalization in three regions (Europe—47%, North America—16%, South America—37%) using the Santander Global Platform (SGP). For example, diversified banks in Spain, such as BBVA and Santander, are compensating for losses by expanding their branches around the world. BBVA Bank focuses on Turkey, Latin America, and the United States, while Santander Bank focuses more on countries with high credit ratings. Spanish banks tend to choose geographic diversification strategies [40]. BBVA has developed its own multi-factor portfolio model for assessing capital for credit risk, taking into account the effects of diversification and concentration in accordance with the requirements of Basel II. Economic capital is sensitive to geographical diversification.

Previous authors used a system model and assessed the impact of risk on the probability of default (Basel standards), and showed that regulation and supervision are important factors for Spanish banks [41]. For the purpose of diversity, it is necessary to introduce new regulation of the financial system as a whole. The modularity assumes a personal design of the interbank network. In USA, modularity is applied if there is the risk of hedging capital.

The use of the Norwegian Bank ID is gaining popularity with the help of a conscious ecosystem cloud and access to the electronic government system using modern applications. In Belgium, this practice is less effective [42]. The practice of sectoral and geographical diversification of 40 banks shows, based on the analysis of ROA (return on assets) and ROE (return on equity) and using the Herfindahl Index, that these indicators are consolidated through diversification. Diversification of a loan increases risks and does not increase profits, although this statement is individual for each country [43].

A study using econometric models of shareholders of European Union banks has shown that larger shareholders have more diversified portfolios and are softer in management and also take more risks. In countries with restrictive regulation, there is a decrease in risks and shareholders [44]. Studies conducted in Spain, using the Haversine formula and an econometric model, show that geographical diversification may not affect risks, and further developments may be in conjunction with cultural factors for banks in other countries [45]. Analysis with the use of a sample of data from Asian countries, in contrast to studies of the USA and Europe, proves an increase in the efficiency of banks through diversification [46]. Geographical risk negatively affects the value of the bank's shares; however, this risk can be minimized if the bank stops opening additional branches, especially due to the development of mobile banking [47]. The results of the regression model of geographical factors and regulatory supervision do not affect the process of market assessment of banks [48].

According to a 2019 survey, medium and large e-commerce companies experienced DDoS attacks (34%) and hacks (26%), while 10% did not have cybersecurity incidents. To protect themselves from DDoS attacks, 42% used a hardware solution, while 18% began filtering network services [49]. In Spain, cybersecurity is a priority for financial institutions that are more than 200 points in the security rating below the average European rating. Therefore, there is a need to invest in cyber risk and security management [50–52]. Banks around the world have more cybercrime risks than other companies, hence financial institutions should pay attention to cyber security [53]. FinTech companies can improve their competitiveness and affordability of their products through a widespread use of apps, and thus mediation costs can be lowered [54]. In the future, banks need to upgrade platforms and their operations in the context of digitalization in order to strengthen management methods, reduce operational risk, and improve organizational structure and operational risk insurance management.

5. Conclusion

The analysis of the diversification of world banks shows that in practice a set of strategies and methods of risk management should be applied to achieve sustainable development of the financial system. Studying the customers of banks and their needs in modern society requires constant international communication and the development of partnerships in order to create the conditions necessary for the provision of safe financial services and sustainable growth of banks. The authors applied ORM to optimize risk management in bank digitization for Santander Bank of Spain. This approach to measurements (AMA) under Basel II and in the context of monitoring and risk assessment allowed the authors to identify the following potential threats: the threat of defects and failures; the threat of loss of data integrity and unauthorized access to customer data; the threat of a violation of the technical system in the information space; and the threat of cyberattacks. The ratio of the total minimum value of operational risk to the total capital of the bank was 0.65%, which is below the permissible minimum value and is acceptable. Accordingly, the authors identified chose a mechanism of bank risk management, diversification of business risks, in order to increase sustainability.

The diversification of banking risks in sustainable financing also has a positive effect on the capitalization of banks. Diversification of risks will allow banks to increase cash flows and receive additional income. For the development of socio-economic activity, the digitalization of banking processes is important in order to create new economic relations and stimulate development. However, in the context of digitalization, the threat of cyberattacks creates problems for customers and undermines the reputation of banks. In the context of globalization, financial institutions need to attract additional

investments to manage cyber risks and build relationships with stakeholders to exchange information and cover the risks associated with cyberattacks, and thereby contribute to sustainable growth of finances.

In further studies, attention will be paid to the processes of digitizing banking services from the customers' point of view and identifying factors that determine their satisfaction with the use of digital services in managing accounts. This will allow the authors to assess whether the banks' products are in line with customer expectations and to propose ways to transform banks' operations in order to strengthen financial stability of the latter.

Author Contributions: The individual responsibilities and contribution of the authors are listed as follows: F.Z.A. worked on the original idea. F.Z.A. and B.Š. performed the detailed conceptualization and investigation of this research. B.Š. finalized the methodology and data analysis of this research. F.Z.A. performed the write-up of this project, including the writing of original draft. F.Z.A. and B.Š. performed the data collection and data analysis. F.Z.A. and B.Š. wrote the final draft and conducted the review, proofreading, and editing for final submission. F.Z.A. coordinated the methodology and data analysis stage of this research project. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ruinan, L. Comparison of Bank Efficiencies between the US and Canada: Evidence Based on SFA and DEA. *J. Compet.* **2019**, *11*, 113–129.
2. ING Bank. Ecosystems: The Future for Banks? 2020. Available online: <https://view.ingwb.com/ecosystems-the-future-for-banks> (accessed on 5 April 2017).
3. Carbó-Valverde, S.; Cuadros-Solas, P.J.; Rodríguez-Fernández, F. The Effect of Banks' IT Investments on the Digitalization of their Customers. *Glob. Policy* **2020**, *11*, 9–17. [[CrossRef](#)]
4. Rahman, A.; Rozsa, Z.; Cepel, M. Trade Credit and Bank Finance—Evidence from the Visegrad Group. *J. Compet.* **2018**, *10*, 132–148. [[CrossRef](#)]
5. Institute of International Finance. The Future of Risk Management in the Digital Era. McKinsey&Company Report. 2017. Available online: <https://www.mckinsey.com/~{}media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ashx> (accessed on 5 April 2017).
6. Santander Consumer Bank. 2018 Pillar 3 Disclosures Report. 2018. Available online: <https://www.santander.com/content/dam/santander-com/en/documentos/hechos-relevantes-c-n-m-v-/2019/02/HR-2019-02-28-2018%20Pillar%203%20Disclosures%20Report-en.pdf> (accessed on 5 April 2017).
7. Moudud-UI-Huq, S.; Ashraf, B.N.; Gupta, A.D.; Zheng, C. Does bank diversification heterogeneously affect performance and risk-taking in ASEAN emerging economies? *Res. Int. Bus. Financ.* **2018**, *46*, 342–362. [[CrossRef](#)]
8. Khan, S.J.M.; Samsudin, S.; Islam, R. Efficiency of banks in Southeast Asia: Indonesia, Malaysia, Philippines and Thailand. *Int. J. Soc. Econ.* **2017**, *44*, 2302–2312. [[CrossRef](#)]
9. Do, H.T.K.; Chu, L.K.; Nguyen, P.M. Vietnamese Banking System in the Context of ASEAN Financial Integration. *Int. J. Financ. Res.* **2017**, *8*, 155–165. [[CrossRef](#)]
10. Taskinsoy, J. Asian Miracle, Asian Tiger, or Asian Myth? Financial Sector and Risk Assessment through FSAP Experience: Enhancing Bank Supervision in Thailand. *SSRN Electron. J.* **2019**, *1*, 1–24. [[CrossRef](#)]
11. Syadullah, M. ASEAN banking efficiency review facing financial services liberalization: The Indonesian perspective. *Asian Develop. Policy Rev.* **2018**, *6*, 88–99. [[CrossRef](#)]
12. Cortés, K.R.; Strahan, P.E. Tracing out capital flows: How financially integrated banks respond to natural disasters. *J. Financ. Econ.* **2017**, *125*, 182–199. [[CrossRef](#)]
13. Gilje, E.P.; Loutskina, E.; Strahan, P.E. Exporting liquidity: Branch banking and financial integration. *J. Financ.* **2016**, *71*, 1159–1184. [[CrossRef](#)]
14. Levine, R.; Lin, C.; Xie, W. *Geographic Diversification and Banks' Funding Costs (No. w22544)*; National Bureau of Economic Research: Cambridge, MA, USA, 2016.

15. Dvorsky, J.; Popp, J.; Virglerova, Z.; Kovács, S.; Oláh, J. Assessing the importance of market risk and its sources in the SME of the Visegrad Group and Serbia. *Adv. Decis. Sci.* **2018**, *22*, 1–22.
16. Oláh, J.; Kovács, S.; Virglerova, Z.; Lakner, Z.; Kovacova, M.; Popp, J. Analysis and comparison of economic and financial risk sources in SMEs of the Visegrad group and Serbia. *Sustainability* **2019**, *11*, 1853. [CrossRef]
17. Doerr, S.; Schaz, P. Bank loan supply during crises: The importance of geographic diversification. *BIS Work. Pap.* **2019**, 827. [CrossRef]
18. Cai, W.; Xu, F.; Zeng, C. Geographical diversification and bank performance: Evidence from China. *Econ. Lett.* **2016**, *147*, 96–98. [CrossRef]
19. Bömer, M.; Maxin, H. Why fintechs cooperate with banks—Evidence from Germany. *Zeitschrift Gesamte Versicherungswissenschaft* **2018**, *107*, 359–386. [CrossRef]
20. Panja, B.; Fattaleh, D.; Mercado, M.; Robinson, A.; Meharia, P. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 20–24 May 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 397–403.
21. Hryshchuk, R.; Yevseiev, S. The synergetic approach for providing bank information security: The problem formulation. *Inf. Secur.* **2016**, *22*, 64–74.
22. Belás, J.; Korauš, M.; Kombo, F.; Korauš, A. Electronic banking security and customer satisfaction in commercial banks. *J. Secur. Sustain. Issues* **2016**, *5*, 411–422.
23. Servidio, J.S.; Taylor, R.D. Safe and Sound: Cybersecurity for Community Banks. *J. Tax. Regul. Financ. Inst.* **2015**, *28*, 5–14.
24. Crisanto, J.C.; Prenio, J. Regulatory Approaches to Enhance Banks' Cybersecurity Frameworks. *Financ. Stab. Inst. (FSI) Insights Policy Implement.* **2017**.
25. Camillo, M. Cybersecurity: Risks and management of risks for global banks and financial institutions. *JRMFI* **2017**, *10*, 196–200.
26. Gaur, A.; Ondrus, J. The role of banks in the mobile payment ecosystem: A strategic asset perspective. In Proceedings of the 14th Annual International Conference on Electronic Commerce, Singapore, 6 August 2012; pp. 171–177.
27. Tinnilä, M. Impact of future trends on banking services. *J. Internet Bank. Commer.* **2012**, *17*, 1–15.
28. Maixé-Altés, J.C. The digitalization of banking: A new perspective from the European savings banks industry before the Internet. *Enterp. Soc.* **2019**, *20*, 159–198. [CrossRef]
29. Samar, S.; Ghani, M.; Alnaser, F. Predicting customer's intentions to use internet banking: The role of technology acceptance model (TAM) in e-banking. *Manag. Sci. Lett.* **2017**, *7*, 513–524.
30. Susanto, A.; Chang, Y.; Ha, Y. Determinants of continuance intention to use the smartphone banking services. *Ind. Manage. Data Syst.* **2016**, *116*, 508–525. [CrossRef]
31. Chaikovskiy, Y.; Kovalchuk, Y. Banking innovations: Perspectives and threats of electronic banking services. *World Financ.* **2019**, *4*, 121–136.
32. Shrier, D.; Canale, G.; Pentland, A. *Mobile Money & Payments: Technology Trends*; Massachusetts Institute of Technology: Cambridge, MA, USA, 2016.
33. Ahmed, J.M. A conceptual framework for the Basel accords-based regulation. *J. Financ. Regul. Compliance* **2016**, *24*, 90–103. [CrossRef]
34. Teplý, P. The application of extreme value theory in operational risk management. *Ekon. Cas.* **2012**, *60*, 698–716.
35. Joshi, D.; Parihar, S. Digitalization & Customer Perception towards the Banking Services. *Aweshkar Res. J.* **2017**, *33*, 133–141.
36. Japparova, I.; Rupeika-Apoga, R. Banking business models of the digital future: The case of Latvia. *Eur. Res. Stud.* **2017**, *20*, 846. [CrossRef]
37. KPMG. *Global Banking Fraud Survey*; KPMG Report; KPMG: Amstelveen, The Netherlands, 2020; Available online: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf> (accessed on 17 February 2020).
38. Shestak, V.A.; Volevodz, A.G.; Alizade, V.A. On the possibility of doctrinal perception of artificial intelligence as the subject of crime in the system of common law: Using the example of the U.S. criminal legislation. *Russ. J. Crim.* **2019**, *13*, 547–554. (In Russian) [CrossRef]

39. Vrbančić, G.; Fister, I., Jr.; Podgorelec, V. Parameter Setting for Deep Neural Networks Using Swarm Intelligence on Phishing Websites Classification. *Int. J. Artif. Intell. Tools* **2019**, *28*, 1960008. [CrossRef]
40. Stewart, J. Who is Going to Save Spain's Savings Banks? *The Banker*. 2012. Available online: <https://www.thebanker.com/World/Western-Europe/Spain/Who-is-going-to-save-Spain-s-savings-banks?ct=true> (accessed on 5 April 2017).
41. Gómez-Fernández-Aguado, P.; Parrado-Martínez, P.; Partal-Ureña, A. Risk Profile Indicators and Spanish Banks' Probability of Default from a Regulatory Approach. *Sustainability* **2018**, *10*, 1259. [CrossRef]
42. Eaton, B.; Hallingby, H.K.; Nesse, P.J.; Hanseth, O. Achieving Payoffs from an Industry Cloud Ecosystem at BankID. *MIS Q. Executive* **2014**, *13*, 223–235.
43. Turkmen, S.Y.; Yigit, I. Diversification in banking and its effect on banks' performance: Evidence from Turkey. *Am. Int. J. Contemp. Res.* **2012**, *2*, 111–119.
44. García-Kuhnert, Y.; Marchica, M.T.; Mura, R. Shareholder diversification and bank risk-taking. *J. Financ. Intermed.* **2015**, *24*, 602–635. [CrossRef]
45. Anderson, B. *Is Geographic Diversification Associated with Increased Risk? Evidence from the Spanish Banking Crisis*; Ursinus College: Collegeville, PA, USA, 2014.
46. Lee, C.C.; Hsieh, M.F.; Yang, S.J. The relationship between revenue diversification and bank performance: Do financial structures and financial reforms matter? *Jpn. World Econ.* **2014**, *29*, 18–35. [CrossRef]
47. Aguirregabiria, V.; Clark, R.; Wang, H. Diversification of geographic risk in retail bank networks: Evidence from bank expansion after the Riegle-Neal Act. *RAND J. Econ.* **2016**, *47*, 529–572. [CrossRef]
48. Guerry, N.; Wallmeier, M. Valuation of diversified banks: New evidence. *J. Bank. Financ.* **2017**, *80*, 203–214. [CrossRef]
49. TADVISER. Information Security in E-Commerce. 2019. Available online: http://tadviser.com/index.php/Article:Information_security_in_e-commerce (accessed on 5 April 2017).
50. ElevenPaths. *The State of Cyber Risk in Spain*; Telefonica: Madrid, Spain, 2018; Available online: <https://business.blogthinkbig.com/cyber-risk-spain-cybersecurity/> (accessed on 5 April 2017).
51. Redo, M.; Siemiątkowski, P. Cost channel in the mechanism of transmitting monetary policy in Poland. *J. Int. Stud.* **2019**, *12*, 130–143. [CrossRef]
52. Shkolnyk, I.; Kozmenko, S.; Kozmenko, O.; Mershchii, O. The impact of the economy financialization on the level of economic development of the associate EU member states. *Econ. Sociol.* **2019**, *12*, 43–58. [CrossRef]
53. Tariq, N. Impact of cyberattacks on financial institutions. *J. Internet Bank. Commer.* **2018**, *23*, 1–11.
54. Aaron, M.; Rivadeneyra, F.; Sohal, S. *Fintech: Is This Time Different? A Framework for Assessing Risks and Opportunities for Central Banks (No. 2017-10)*; Bank of Canada Staff Discussion Paper; Bank of Canada: Ottawa, ON, Canada, 2017.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).