International Social Sciences and Humanities
UMJember Proceeding Series (2023) Vol. 2 No 3: 1433-1443

Proceedings of the ICON 2023
International Conference

Enterprise Risk Management Implementation for Digital Banking During Covid-19 Partial Lockdown In Indonesia

Krisna Damayanti[1]*, Basuki[2]

[1]Doctoral Program Faculty of Economics and Business, Universitas Airlangga Surabaya

[2]Sekolah Tinggi Ilmu Ekonomi Indonesia Surabaya

*Correspondence: Krisna Damayanti
Email: krisna.damayanti-019@feb.unair.ac.id

Accepted: July 2023
Published: September, 2023

Abstract: To explore the detail of operational risk faced by digital banking during the Covid-19 pandemic in Indonesia, including the highest Delta variant outbreak in the worldwide; and at the same time, to explore the most efficient and effective strategies to minimize the operational risk. **T**his research uses qualitative methods, namely interviews and documentation through public social media. Digital banking did not use innovative strategies to overturn and tackle the existing strategies before the pandemic occurred, and the banking sector tended only to update the strategies by strengthening, maximalising and optimalising facilities due to the increasing usage of mobile and internet banking. Due to the Covid-19 pandemic, this research has tended to utilise online interviews through social media with less meetings in person meaning there is a lack of information about the gestures and signal of respondents. Operational risk defines deeper innovative strategies to tackle the larger and wider scope of implementation digital banking in Indonesia. The banking needs to optimise the updating system through empowering and strengthening how it tackles the bigger operational risks thar come with bigger volume and the same operational risk patterns in the Indonesian context. Society could be enlightened on the best way of engaging in working from home and working from the office for the purposes of social distancing to avoid spreading Covid-19 thus reducing the risk of death. Using qualitative research methods, the identification and measurement of operational risk, and how to avoid it, from the perspective of Enterprise Risk Management, when implementing digital banking in the era of the Covid-19 pandemic as a result of implementing a partial lockdown in Indonesia.

Keywords: enterprise risk management, covid-19, partial lockdown (PPKM), digital banking, mobile banking

INTRODUCTION

An arrangement called “Work From Home” (WFH) was an impact of the Covid-19 pandemic and was a kind of restriction of social activities carried out in various sectors, especially in the crucial banking sector. The banking system in Indonesia has now begun to expand its facilities so that its customers can obtain various kinds of services independently (self-service) without them needing to visit the bank office to carry out various types of transactions (cash, payments, transfers) and avail themselves of various other services including closing accounts. These digital services are collectively referred to as digital banking [19]. The digital banking system, through internet banking and mobile banking, is the main tool employed by banking businesses in the era of Covid-19 in supporting Community Activities Restrictions Enforcement or CARE (Indonesian acronym: PPKM).

In maximising their services to customers, banking service providers need to develop a digital banking system that is able to meet customer needs by making full use of banking resources [7], [17]. The implementation of WFH, in the context of the social restrictions on the community in order to

break the chain of the spread of Covid-19, needs to be supported through the provision of banking services for customers so they can continue to carry out productive activities in terms of banking. For this, the banking sector needs to perfect a suitable digital banking system for the Indonesian people, especially one that is able to integrate with the global system in order to carry out international financial activities, especially those related to banking [7].

The impact of the Covid-19 pandemic on banks saw an increase in the volume of banking transactions, so the existence of the digital banking implemented by banks greatly assisted banking activities in the PPKM era. The implementation of a digital banking system that was in accordance with customer needs would significantly improve customer performance. The banking service provider needed to identify and measure the operational risks of digital banking services which were an obstacle to banking so that they could review, revise and update the digital banking service system so that it was appropriate, effective and efficient.

How was the exploration conducted by digital banking service providers—namely the banks—able to identify and measure the operational risks of an effective and efficient digital banking service in order to optimalise it for both the banking industry and the customers while also being able to optimalise the use of the resources owned by service providers in the Covid-19 pandemic era during the implementation of PPKM (Partial Lockdown) in Indonesia?

An effective and efficient corporate strategy needed to be established in order to be capable of winning in the face of rapidly increasing business competition [6]. This necessitated creating a digital banking system, involving both internet banking and mobile banking, that was more updated so that it could support the activities of the banking sector in Indonesia in the era of Covid-19 and minimise operational risk. Banks provided a digital banking system, both internet banking and mobile banking, that was able to meet the needs of customers as digital banking users during the Covid-19 pandemic era when PPKM was being implemented in Indonesia.

Using qualitative research methods, this study explores the identification, measurement and avoidance of operational risk using an Enterprise Risk Management (ERM) system in the implementation of digital banking in the era of the covid-19 pandemic and as a result of implementing PPKM in Indonesia. Banks have a goal to improve the quality of banking services to customers. The implementation of online banking in Indonesia is in line with the increasing number of users of mobile device which have become part of people's lifestyles. Observing this situation, the banking sector has provided easier access to services for its customers such as account opening, transfers, bill payments, or other financial planning. online system [18].

This study is able to provide a comprehensive picture for the banking business in opening up new business opportunities as well as facing challenges, especially the digital banking business, and internet banking and mobile banking in particular.

It is able to help by providing initial steps in identifying and measuring the operational risks of digital banking business. This study provides solutions for improving the digital banking system that are suitable for the needs of customers, and are effective and efficient for digital banking. This study supports government activities, in this case PPKM, which limit movement and social restrictions in the community to break the chain of the spread of Covid-19.

Research conducted by [19] found that the banks BCA and BRI have low operational risk according to customers who were surveyed. Although BCA is considered to have lower operational risk than BRI, several areas such as system risk need more attention, while research by [17] deals

with the implementation of internet banking risk management. In addition to providing convenience for customers, internet banking also has the potential to increase risk and many previous studies discussing the operational risks of digital banking utilize quantitative research.

However, this study discusses the operational risks of digital banking by exploring it in detail through research using qualitative methods through interviews, FGDs and open questionnaires with users and providers of mobile banking services at Bank BCA, BNI 46, Bank Mandiri, and BRI so as to be able to uncover the crucial factors in perfecting an effective and efficient digital banking system.

METHOD

This study uses qualitative methods to collect information, such as focus group discussions. This approach is considered to be in line with the objectives of this study because it explores, in depth, the operational risk faced by implementing digital banking business amid the PPKM lockdown during the Covid-19 pandemic [24].

Type and source of data

The primary data are those that are directly provided to data collectors [24]. The primary data collected in this study have been obtained directly from respondents or informants through debriefings or interviews. The targeted respondents were bank's middle managers who were able to represent the interests of their banks' top managers; respondents also included lower-level managers who worked in cooperation with the top managers and ensured their policies were carried out.

The indicators, measurements, and dimensions used in previous research [19], which are mostly quantitative research of the same type that discuss banking digital operational risks, have been used: structured, semi-structured, and open-ended questions questionnaires and in-depth interviews. Focus Group Discussions (FGDs) have been developed for this qualitative research by conducting analytical interviews using big data regarding the disclosure of banking constraints in the application of digital banking, in addition to reavealing the architect of digital banking in each bank and how they are concerned by disclosing problems faced, and analysing the pattern of types of transactions and what risks arise, especially in the pandemic era during the implementation of PPKM.

Face-to-face interviews took place at each bank's operational offices, for one hour each, over a period of one day of direct discussions at the central office. The rest of the time, interviews were conducted indirectly through the application "Messenger", or by phone, or email. Most of the interviews were conducted during working hours or depended on the availability of the informants. The duration of each interview depended on whether the respondent had already met with the interviewer. Some were interviewed between two and four times. This study has used abbreviations, instead of the respondents' names, to maintain confidentiality and encourage informants to provide vital information.

According to [25], anonymity "requires that each researcher systematically change the subject's real name to a pseudonym or case number when reporting data". Anonymity is important because the information obtained from each bank respondent may be used in a public or private document, in print or an electronic format [26].

Other data were obtained from documents that provide information on banks' investments for infrastructure and from contracts, codes of ethics, procedures, literature, scientific journals, archives and official documents related to research institutions.

"Purposive sampling" was used to determine which respondents to interview for the qualitative data-gathering process. Purposive sampling is decision-based and depends on the objectives and criteria of the research [27]. The respondents selected through this process were from both Islamic and conventional banks and matched the following criteria:

1) Representatives of one of the four biggest bank in Indonesia [9].
2) Their banks have implemented fully mobile banking and or internet banking

The following are the respondents from respective banks:

Name	Designation	Skills qualification	Unit area
R.S.I.P.	Public relations manager executive	External public relations	Bank Negara Indonesia, Jakarta
M.A.	Account manager executive	Financial	Bank Central Asia, Jombang
K.P.	Operational credit manager executive	Financial systems	Bank Rakyat Indonesia, Surabaya
D.S.	Operational manager executive	Systems Analysist	Bank Mandiri, Surabaya

Research objectives

Forming an architectural design for digital banking systems, both internet banking and mobile banking, that suits customer needs in the Covid-19 pandemic era while providing an effective and efficient digital banking system architecture design for the digital banking business by minimizing operational risk.

Research Road Map

Conceptual framework

The implementation of digital banking throughout the partial lockdown brought with it operational risks for the banking industries. Hence, this research segregates Enterprise Risk Management to manage two risk categories: 1) internal risk and 2) external risk. On one hand, internal risks to be managed are risks that come from inside a bank that include human resource risks, system and technology risks, and physical risks. On the other hand, external risks to be managed include risks that come from outside a bank and these are economic risks, natural risk and political risks. Those risks that come from outside and inside a bank relate to the implementation and existence of digital banking meaning mobile and internet banking as depicted in Figure 2. The relevant risk in this research focus on all the implementation during the Covid-19 pandemic starting from the outbreak in December 2019 until now.

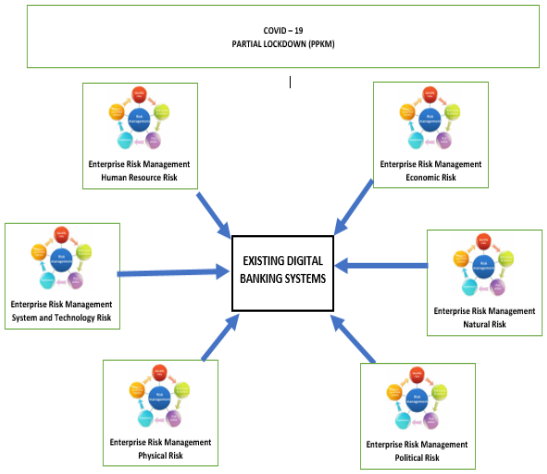

Figure 2. Research Conceptual Framework
Source: Author, 2022

RESULTS AND DISCUSSION

Mobile banking and internet banking are widely available in Indonesia through the implementation of digital banking, but it the existence of digital banking affected and had implications for financial services and domestic stakeholders, especially during the pandemic.

ERM Human Resources Risk

PT Bank Negara Indonesia 46 (BNI 46) continued to strengthen cyber security protection during the development of their digitalization of banking services. The development of digitalization in the banking industry does not have only positive impacts on banks and customers. For example, digitalization is also followed by an increase in the potential for banking crimes. The trend in financial crime is for it to be increasingly technology-based.

One interviewee, hereinafter referred to as RSIP, was the Public Relations Manager at BNI 46; they explained that digital banking crimes took various forms. Among them are the defrauding of customers, namely phishing and spamming, fraud in the form of the misuse of legitimate transactions, attacks in the form of leaking customer data, or attacks on bank systems. BNI 46 has three pillars of cyber security protection—namely the people, process, and technology—that are always being improved to prevent banking crimes.

RSIP also stated that the highest risk came from humans, also known as the people aspect. In accordance with survey studies conducted by various research institutions, people or customers are the weakest points that are most often attacked. For example, customers are deceived by fake call centres or social media as if on behalf of the bank.

RSIP elaborated that, although banks have tried their best to filter with various processes and technologies, customers can still consciously give cell phone numbers, PIN/OTP, and personal data to fraudsters. To prevent this, BNI 46 always carries out briefings/awareness raising and runs a 24-hour call centre.

As for the people pillar, RSIP explained that BNI 46 always improves the professionalism and competence of its employees as customer partners by providing various trainings and cyber security certifications. Meanwhile, customers are always given tips and kept aware regarding the use of safe digital transactions.

For the process pillar, RSIP also confirmed that BNI 46 adheres to a simple and secure process using multilevel verification that can secure funds, transactions, and customer data. This process is always being improved to suit the times, such as anti-fraud automation and layered verification of customer identities.

Regarding the technology pillar, RSIP clarified that this state-owned bank applies the latest security technology in bank products such as Firewall, Cloud-based Security, Anti-Fraud Detection, and the security provided by customer data encryption. BNI 46 also has a system that can maintain the availability of services.

ERM System and Technology Risk

The existence of digital banking, in addition to delivery benefits, similarly has the potential to carry several risks. The first digital banking risks are allowed by consumers, especially data security risks or cyber risks, privacy, along with data ownership and data governance. This risk can ascend due to the vulnerability of computer-based systems and processes that are interrelated and can be

oppressed by hackers for pleasure or criminal intent [15], [22]. Of course, the risks confronted by consumers will also affect operations, i.e. operational digital banking risks, financial market infrastructure, or even sectors that are vulnerable to shocks. Further crystallization of these risks could have a systemic impact on the whole financial system.

The banking system is often an easy target for cyber criminals, the more complete digital services are, the risk of cybercrime will also increase. This indication is reinforced by the latest report released by the National Cyber Security Operations Centre of the National Cyber and Crypto Agency (Indonesian acronym: BSSN). According to the institute, in 2020 there were 495 million cyber-attacks. That number is up five times compared to the previous year which saw 228 million cyber-attacks.

In terms of the various cyber-attacks that have occurred globally, the financial sector is the sector most frequently affected. “Cyber-attacks targeting the banking sector have an economic motive with the perpetrators being cybercriminals. Various cases in Indonesia have also often involved bank burglary using cyber-attacks by utilizing social engineering, OTP fraud, SIM swaps, weaknesses in the banking system and phishing," explained the BSSN’s Director of Vulnerability Identification and Risk Assessment of National Critical Information Infrastructure, the interviewee hereinafter referred to as IR. Previously, the World Economic Forum had also released the Global Risk Report 2021 which said that the risk of cyber-attacks was still one of the highest risks, although it was still below the risk of natural disasters, environmental damage and infectious diseases.

Furthermore, IR from BSSN noted that, throughout 2020, the most frequent cyber incidents occurred in the form of malware, phishing, data theft, disturbed denial of service (DdoS), skimming, jackpotting, and bugs or weaknesses in banking information systems . One of the most common cyber incidents were due to malware, viruses, or trojans. Check Point Research noted that the most common top banking trojans in 2020 were *trickbot, ramnit, ursnif, danabot, dridex,* and *qbot.*

According to IR, cyber-attacks in the form of phishing, malware, trojans, and other attacks that cause incidents, can also be triggered due to a lack of security awareness. Chairman of the Bankers Association for Risk Management, an interviewee hereinafter referred to as ASB, strongly agrees with IR and states that the banking industry was the main target for cyber-attacks during the pandemic. ASB said the banking industry was still the industry most targeted for cyber-attacks with an index of 23 percent, followed by the manufacturing and energy industries.

The most frequent attack variation was ransomware which increased to 23 percent in 2020 from 20 percent in 2019. This kind of attack seeks to encrypt and steal data so that it can be accessed by perpetrators with the aim of demanding a financial ransom. Then, data theft and data leak attacks also increased from 5 percent to 13 percent in 2020. These kinds of attack seek to take advantage of sensitive data such as banking login credentials. In addition, there are also server access attacks whose index has increased from 3 percent to 10 percent in 2020. This kind of attack attempts to access important data with unauthorized accounts. Next, there is a form of remote access trojan attack, whose index rose from 2 percent to 6 percent. This is an attack involving malware that serves as a backdoor to control a bank system.

Meanwhile, BSSN’s IR also reminded the interviewer that the incidence of attacks in the banking sector sees them being more often targeted at internet banking and mobile banking applications. Various methods are used by hackers to exploit vulnerabilities in internet banking and mobile banking application business processes.

With the development of cyber threats in the banking sector, IR completed a cyber risk profile in the banking sector in 2020 with the scope of internet banking and mobile banking. IR hoped that the preparation of the cyber risk profile can be used as a reference focus for the banking industry to be able to mitigate potential cyber threats and vulnerabilities.

BSSN's 2020 survey on the Banking Sector Risk Profile categorized four risk levels, namely very high, high, medium, and low. These risk levels were categorized based on the impact scale and likelihood scale of each identified risk. IR explained that these various risk profiles can have a very significant impact on the organization if they occur, especially related to operational and financial impacts. "Factors that cause this potential risk can come from internal or external parties of the company. Internally, fraud can be caused by lack of testing, lack of control and monitoring, or other factors. Meanwhile, external parties are related to the lack of security awareness from customers according to IR. BSSN's IR also identified the profile of threats and vulnerabilities of mobile banking and internet banking services in Indonesia throughout 2020. This is considering that these two services are the most widely used in digital banking services in the Indonesian banking sector in conducting financial transactions.

It was revealed that the threats to the mobile banking system that there were in 2020 included abuse of access rights, phishing attacks on customers, data theft, application mismanagement, malware attacks, and sim card hijacks. IR explained that every threat to mobile banking can be a risk if one or more vulnerabilities are found that can trigger the threat. Although cyber-attacks continue to increase from year to year in the financial sector, the mitigation carried out by banking business actors has not been in line with the threatening risks. According to IR, the mitigation or management of cyber security risk reduction has the lowest rank in Indonesia's banking operational management strategy.

Therefore, IR reminded the interviewer that mitigation to anticipate the risk of cyber-attacks is something that must be carried out to prevent an increase in cyber-attacks against banks and financial institutions. This is especially the case in this new normal era where digital transformation in various fields is encouraged. Cyber threats and vulnerabilities in the banking sector can come from the consumer or organizational side. Consumers can experience the crimes involving ATM cards and mobile banking, while organizations experience vulnerabilities in DDoS, so Application Programming Interfaces (APIs) must be secured according to IR.

IR concludes that, despite the high number of cyber-attacks on the financial sector, BSSN still participates in the cyber security protection of the financial sector through regulations and protection services. BSSN implements an information security index to prevent the risk of cyber-attacks that can weaken financial and banking organizations. Responding to this, ASB explained that banks continued to strengthen risk management governance during the pandemic period 2020-2021. In fact, mitigation efforts are even more intense and in line with the increasing intensity of cyber-attacks amid digital transformation carried out by many banks. ASB also found that banking is directly related to data, and the amount of people's savings. After banking, the manufacturing and energy industries are new.

ERM Physical Risk

PT Bank Central Asia Tbk. (BCA) acknowledges that it prioritizes risk mitigation for consumer protection, especially in its digital services. Director of BCA, and interviewee hereinafter

referred to as S, explained that consumer protection is a very high priority, given the role of banks as a trust-based business institution. BCA acknowledges that it always applies risk management principles to avoid digital crimes. The weakness is often on the customer side, so this is related to consumer protection. However, in Indonesia, cybercrimes that occur, even if there is fraud, are not a sophisticated kind of fraud, so BCA also continues to educate customers.

This private bank, which has the largest assets, is considered one of the most advanced in terms of its digital services. From the start, the electronification of banking services has been BCA's focus as the company pursued cost efficiency through digital banking. Interviewee S stated that the company's investment in information technology (IT) is the largest allocation in its investment budget. In addition to IT investment, the other largest allocation is investment in operations because it is recognized that there are still processes in bank services that have not been digitized.

ERM Economic Risk

For financial services, digital banking has the potential to lead to an "unbundling" and restructuring of existing financial services. The existence of digital banking can "break" the concentration that arises in the financial market thus market share will be scattered among competitors who offer the same services. As a result, there is no longer the dominance of certain financial intermediary institutions in the financial market and the competition that happens has the potential to lower the price level of financial services.

In addition, digital banking will also change the contestability in financial services since of the relatively low cost for new entrants to enter the market [11]. With the breakdown of market concentration and changes in the contestability of financial services, the composition or structure of financial services will also change. These changes, apart from opening up opportunities for diversification and decentralization, also have the potential to boost efficiency in the financial system. An equally important implication for the financial system is the creation of transparency so that it can reduce—if not eliminate—asymmetric information and improve the ability of market participants to manage risk.

The existence of digital banking opens up greater opportunities for consumers, households, and the business world, including small and medium enterprises (SMEs), to access financial services. In addition, digital banking also offers convenience, speed of service, and lower costs as well as convenience for consumers in enjoying financial services. The most important implication and dividend of the various benefits of digital banking is financial inclusion. This is further expected to promote sustainable economic growth and enable diversification of exposure to overall investment risk.

ERM Natural Risk

The transformation of financial services towards being digital was increasingly massive during the Covid-19 pandemic. Restrictions on individual mobility forced people to use online services to fulfil their daily needs. In the banking sector, the policy of social restrictions encouraged the digitization of services which had been echoed several years earlier.

ERM Political Risk

Government Works to Increase Digital Banking Effectiveness and Efficiency

With these implications, the role of the regulator becomes central, especially in designing and implementing proportional financial regulations. The existence of digital banking requires regulation that is no longer solely dependent on entities/intermediaries—namely entity-based regulations and/or activities, namely activity-based regulations—but that instead provides a greater proportion of activity-based regulations. The steps taken by the Financial Services Authority (OJK) by issuing its Regulation No.77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services, can be seen as initial evidence of a special proportion of activity-based financial service regulations in Indonesia. However, the purpose of the OJK's regulation is broader. Besides being intended to protect consumer interests related to the security of funds and data, it also aims to protect national interests related to the prevention of money laundering activities, financing of terrorism, and financial system stability.

On the other hand, Bank Indonesia has also set regulations for digital banking operators whose activities are related to the payment system. This is stated in Bank Indonesia Regulation (PBI) No.19/12/PBI/2017 concerning the Implementation of Financial Technology and its implementation provisions in the Regulation of Members of the Board of Governors (PADG) No. 19/14/PADG/2017 concerning Financial Technology Regulatory Sandbox and PADG No. 19/15/PADG/2017 concerning Procedures for Registration, Submission of Information, and Monitoring of Financial Technology Operators. One of the important points contained in the regulation is the stipulation of the obligation of digital banking operators in the field of financial payment system services to register with Bank Indonesia. In addition, operators are required to conduct limited trials of the technology used for service products and/or financial business models in the regulatory sandbox. This regulatory sandbox approach helps regulators to understand the risks that may arise if a digital banking product is widely used, but in a controlled environment.

This will help digital banking providers, especially start-ups, to test products without having to bear the full regulatory costs or face law enforcement action. The substance of these regulations is, of course, to ensure that digital banking operators do not "run fast and break things". With these various regulations, it is hoped that a healthy digital banking ecosystem will be created to support sustainable and inclusive national economic growth, while maintaining monetary stability, financial system stability, and an efficient, smooth, safe and reliable payment system.

CONCLUSION

Covid-19 has caused disruption and even collapse in societies all around the globe. Every country had to cope with their strength and weaknesses as they tackled the problems that arose because of pandemic. This was to overcome the spread of the virus, especially the Delta variant, that caused the death of thousands of people.

The Indonesian government implemented PPKM and in doing so there were mechanisms that had to be implemented by many individuals and organisations throughout society. Many businesses had to institute WFH or WFO. Many essential businesses in the banking sector had to implement WFO while most of their customers were implementing WFH. The implementation of WFH caused the usage of digital banking, especially mobile and internet banking, to increase. Making bank

transactions at home became the best way to do business without going to bank, engaging in social distancing, and avoiding meeting with many people.

Therefore, the banking sector faced many kinds of risk in updating their digital banking system to optimise it to the needs of customers and, at the same time, to comply with government rules and regulations aimed at minimising of spread of the Covid-19 virus. The most dominant risk that the digital banking sector had was operational risk. Mitigation of the operational risks of digital banking was set up using the most effective and efficient Enterprise Risk Management strategy, especially during the pandemic era, to minimize the internal and external risks.

REFERENCES

[1] Basuki and M. D. Riediansyaf. (2014). The Application of Time Driven Activity-Based Costing in the Hospitality Industry: An Exploratory Case Study. *Journal of Applied Management Accounting Research (JAMAR)* 12 (1), 27.

[2] Basel Committee on Banking Supervision (BCBS). (1974). *Revised international capital framework for monetary and financial stability*. Bank for Internasional Settlement.

[3] Basel Committee on Banking Supervision (BCBS). (2004). *Financial Disclosure In The Banking, Insurance And Securities Sectors: Issues And Analysis*. Bank for Internasional Settlement.

[4] Chartered Global Management Accountant (CGMA) (2013). Report from Insight to Impact: Unlocking Opportunities in Big Data. *http://www.cgma.org/Resources/Reports/DownloadableDocuments/From_insight_to_impact unlocking_the_opportunities_in_big_data.pdf*

[5] Damayanti, K., & Ardini, L. (2015). Auditor with the Javanese Characters and Non-Javanese in Audit Firm: Conflict of Interest. *International Journal of Economics and Management Engineering*, *9*(1), 287-292.

[6] Damayanti, Krisna and Soewarno, Noorlailie. (2021). Never Lose the War throughout Accounting Strategy. *Journal of Hunan University (Natural Science)* 48(6).

[7] Damayanti, K., and Setyawardani, L. (2019). Alliance Cooperation Joint ATM Network: Exploring The Banking Sector In Indonesia. *Qualitative Research in Financial Markets*.

[8] Damayanti, K. (2005). *Pengaruh pengumuman deviden terhadap fluktuasi abnormal return* (Doctoral dissertation, Universitas Gadjah Mada).

[9] Dana Pihak Ketiga (DPK). (2021). *Peningkatan Perhimpunan Dana Pihak Ketiga Semester I-2021*. *https://t.me/kompascomupdate*.

[10] Handayani, N, L. Ardini, and K. Damayanti. (2016). Self-Help Groups (SHGS) Potential and Strategy in Increasing Local Product Quality Through Sub- Contract Model To Maximize Income.

[11] He, D., *et al*. (2017). Fintech and Financial Services: Initial considerations. *IMF Staff Discussion Notes* 17(05).

[12] IBFG Institute. (2018). Enterprise Risk Management (ERM). Retrieved 3 28, 2021, from IBFG Institute. *https://ibfgi.com/enterprise-risk-management-erm/*

[13] King. L, J. (2001). *Operational Risk: Measurement and Modelling.* John Wiley & Sons

[14] Menteri Dalam Negeri Republik Indonesia. (2021). *Instruksi Menteri Dalam Negeri Nomor 24, 26, 27 Tahun 2021 Tentang Pemberlakuan Pembatasan Kegiatan Masyarakat Level 4, Level 3, Dan Level 2 Corona Virus Disease 2019 Di Wilayah Jawa Dan Bali.* Kementerian Dalam Negeri Jakarta Indonesia.

[15] Narain, A. (2016). Two faces of change. *Finance & Development* 53(3).

[16] Otoritas Jasa Keuangan. (2016), (2017). *Peraturan Otoritas Jasa Keuangan Nomor /Pojk.03/2017 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum.*
[17] Priatno, Nurdin, and Maulisa. (2014). *Penerapan Manajemen Risiko Internet Banking Pada Bank Umum Terkait Perlindungan Hukum Bagi Bank dan Nasabah (Studi di Bank X).*
[18] Sakti, A. A., K. Kustantinah and R. W. Nurcahyo (2018). In Vitro and in Vivo Anthelmintic Activities of Aqueous Leaf Infusion of Azadirachta indica against Haemonchus contortus. *Tropical Animal Science Journal*, *41*(3), 185-190.
[19] Tanic, R.H and A.D.R. Atahau. (2021). *Digital Banking dan Risiko Operasional (Studi Kasus Pada Nasabah Bank Central Asia Dan Bank Rakyat Indonesia).*
[20] Wurintara, G. Giffari and Hamidah. (2020). The Existence of Accrual Anomaly Phenomena in Indonesia Capital Market. *Journal of Accounting and Investment* 21(2).
[21] World Health Organization, 2020. *Risk Communication and Community Engagement Readiness And Response To Coronavirus Disease (COVID-19).* Interim guidance 19 March 2020.
[22] Wellisz, C. (2016). The Dark Side of Technology. *Finance & Development* 53(3).
[23] Shinhanbank Indonesia. 2000. Company Profile Articles.
[24] Sugiyono. 2007. Metodologi Penelitian Bisnis. PT Gramedia Jakarta.
[25] Berg, B.L. (2007). Qualitative Research Methods for the Social Sciences, Pearson/Allyn & Bacon
[26] Creswell, J.W. (2007). Qualitative Inquiry and Research Design Choosing among Five Approaches. (2ndedn.), Sage Publication.
[27] Kozak, S. (2005). "The role of information technology in the profit and cost efficiency improvements ofthe banking sector",Journal of Academy of Business and Economics, Vol. 5 No. 2, pp. 1-9.