Bulletin of Monetary Economics and Banking

Volume 20 | Number 3 Article 5

1-31-2018

Online Banking Implementation: Risk Mapping Using ERM Approach

Mochamad Aji Jaya Sakti
Bogor Agricultural University

Noer Azham Achsani
Bogor Agricultural University, achsani@yahoo.com

Ferry Syarifuddin
Bank Indonesia - Indonesia, ferry.s@bi.go.id

Recommended Citation
Jaya Sakti, Mochamad Aji; Achsani, Noer Azham; and Syarifuddin, Ferry (2018) "Online Banking Implementation: Risk Mapping Using ERM Approach," *Bulletin of Monetary Economics and Banking*: Vol. 20: No. 3, Article 5.
DOI: https://doi.org/10.21098/bemp.v20i3.824
Available at: https://bulletin.bmeb-bi.org/bmeb/vol20/iss3/5

ONLINE BANKING IMPLEMENTATION: RISK MAPPING USING ERM APPROACH

Mochamad Aji Jaya Sakti[1], Noer Azam Achsani[2], Ferry Syarifuddin[3]

ABSTRACT

The implementation of online banking in Indonesia is in line with the increasing of mobile device users who have become a part of people's lifestyle, hence online banking offers easiness to access on banking services. This study is to examine risk mapping on the implementation online banking using ERM approach, including risk mitigation strategies for identified risks. This research was conducted at XYZ Bank who has implemented online banking. The results of this study find 55 potential risks. Some of it identified risks related to bank system security such as vulnerability to viruses, malware, hacking, also access information by an unauthorized person. Risk mitigation strategies applied by XYZ Bank is mostly done by managing the risk because the implementation online banking is still on the development process, and the Bank remains optimistic with the future prospect of online banking by staying with government regulations.

Keywords: Risk, Banking, Online Banking, ERM
JEL Classification: D81, G21, O33, Q55

1. School of Management and Business, Bogor Agricultural University, Indonesia.
2. Departement of Economics and School of Management and Business, Bogor Agricultural University, Indonesia. E-mail: achsani@yahoo.com
3. Senior Economic Researcher, Bank Indonesia Institute, Central Bank of Indonesia. E-mail: ferry.s@bi.go.id

I. INTRODUCTION

Referring to Law Number 10 of 1998 regarding the amendment of Law Number 7 of 1992 concerning banking, the Bank is a business entity that collects funds from the community and distributes it back to the community in other forms in order to improve the living standard of the community. One part of the activities, undertaken by the Bank, is to collect funds from the community and serve the financial transactions of customers. However, the business activities undertaken by the Bank cannot be separated from risks both calculated and unpredicted.

Based on the above phenomenon, it is necessary to manage risk in order to anticipate potential risks in fund management and customer transaction services. Referring to Bank Indonesia regulation Number 11/25/PBI/2010 amendment of PBI Number 5/8/PBI/2003 on May 19, 2003, concerning the Application of Risk Management for Commercial Banks, there are eight types of risks that must be managed or considered by banks which are the credit risk, market risk, operational risk, liquidity risk, compliance risk, legal risk, reputation risk, and strategic risk.

The phenomenon of the online banking application, in Indonesia, is in line with the increase in mobile device users that have become part of people's life. The online banking offers an easy access to banking services such as account opening, transfer, bill payment, or other financial planning. The emergence of new companies, based on financial technology (fin-tech) in the financial industry competition where they make technological innovations and products very quickly, demand the banking industry to make adjustments in the business processes and infrastructure that were originally processed manually or offline into the automation process or online with the aim of speeding up services to customers and surviving within the competition (Bank Indonesia, 2016). This change in bank services will create good value and customer experience to the eyes of the customers, and with the improvement of infrastructure can be utilized as a supporting tool in online banking risk management.

Compared to the conventional banking services, where the customers or potential customers must approach the Bank to conduct transactions, online banking services are perceived to be easier and more flexible. Changing the manual process to digital allows a more flexible process, where customers who initially have to go to the Bank office, which provides more comfort through the use of channels that work with the Bank (Eistert et al., 2013). The use of online banking technology has potential risks that must be managed and considered by the Bank. Bank Indonesia (BI) and the Financial Services Authority (OJK) acting as regulators in the financial industry apply some rules regarding online banking implementation. Some of these rules are as follows:

1) PBI 9/15/2007 On Implementation of Risk Management in the Use of Information Technology by Commercial Banks, the regulation in the account opening process is set forth in PBI 14/27 / PBI / 2012 concerning the Implementation of Anti Money Laundering and Counter-Terrorism Financing Program for Commercial Banks where Mandatory Commercial Banks must do Customer Due Diligent (CDD) and Enhancement Due Diligent (EDD) towards prospective customers in order to apply Know Your Customer (KYC) principles.

https://bulletin.bmeb-bi.org/bmeb/vol20/iss3/5
DOI: 10.21098/bemp.v20i3.824

2) POJK Number 01/POJK.07/2013 on August 6, 2013, regarding Consumer Financial Services Protection and SE OJK Number 12/SEOJK.07/2014 on Information Submission in The Framework of Product and/or Financial Services Marketing aims at Bank to deliver related information on the financial services used by prospective customers in a transparent manner by explaining the risks attached to each Bank product to be used by the customer.

The scope of this study covers the risk mapping of online banking application with the Enterprise Risk Management (ERM) approach. Stages of the process were undertaken following the eight ERM frameworks which are internal environment, objective setting, event identification, risk assessment, risk response, control, information and communication, and monitoring. The reason for using ERM method in this research is to get a comprehensive picture of the integration process between the Bank's business objectives, the risks inherent in the business process, as well as the risk mitigation strategy chosen to keep the business process running. The expected output of this online banking risk mapping can be useful for the Bank in managing the risk of online banking services.

The second part of this paper presents a literature review related to online banking risks. The third section describes the data and methodology used. The fourth section presents the results of the discussion on online banking risk mapping, while the fifth section presents the conclusions of this study.

II. THEORY

2.1. The Linkage between Risks and Online Banking

The concept of online banking technology is not just a switch from an offline system to an online system, but also provision of both added value and convenience to the community as well as speed in terms of accessing banking services through technology. The online banking combines two parts, namely the external part associated with the customer experience and the internal part associated with operational processes that are effective and efficient (Eistert et al., 2013).

The use of technology in business processes is closely related to risk. The ease of accessing digital information and that of connections through mobile devices lead to growing risks in the use of technology. The balance between risk management and business processes is important where the use of technology should be an opportunity for business growth, while failure in risk management will harm the business (Baldwin & Shiu, 2010).

The broad concept of risk is an essential foundation for understanding risk management concepts and techniques. Studying the various definitions found in the literature is expected to improve the understanding of the concept of risk which becomes increasingly clear. Some of these differences in the definition of risk are due to the fact that the subject of risk is very complex with many different fields causing different understanding. The risk is divided into three senses: possibility, uncertainty, and the probability of an outcome that is different to the expected outcome (Diversitas, 2008). The systematic management of risks is covered in the concept of risk management. Risk management is a strategy that every industry must adapt to anticipate potential emerging losses that include risk identification activities, risk measurement, risk mapping, risk management, and risk control

(Djohanputro, 2008). Risk management also has other objectives such as obtaining greater effectiveness and efficiency by controlling risk in every company activity (Darmawi, 2006).

The risk categories that exist in online banking include transaction risk, compliance risk, reputation risk, and information security risk (Osunmuyiwa, 2013). While the adoption of e-banking will lead to potential operational and reputation risks (Ndlovu & Sigola, 2013). In addition, the authors argue that the potential for fraud and information security risk are some of the biggest challenges in addition to investment costs for e-banking infrastructure that requires a high cost.

One of the risks that arise from the implementation of online banking is the information security. A common problem affecting information security is the lack of a Bank in implementing controls that lead to a loss in terms of privacy, causing misuse of client confidential information that may affect clients trust in transactions using e-banking (Omariba, Masese, & Wanyembi, 2012). Customer knowledge of security in IT is a factor affecting security in internet banking access. The higher the customer knowledge about information security, the more diligent they will be in conducting activities through the internet (Zanoon & Gharaibeh, 2013).

2.2. Online banking risk mapping using the Enterprise Risk Management (ERM) method

Underlying the author's thinking is that (COSO-ERM, 2004) any organization is established to generate value for the stakeholders. All of the organizations face uncertainty and challenges and the function of management is to determine how much uncertainty is received as a compensation for increasing the value of the firm. The framework of the ERM presents four-goal categories and eight components related to corporate entities as the objects of ERM analysis. The four categories of corporate objectives include strategic, operational, reporting, and compliance. Meanwhile, the eight components related to the corporate entity include the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring - all of the ERM activities must be monitored and evaluated as the basis of subsequent development.

(Cormican, 2014) in his research on "Integrated Enterprise Risk Management: From Process to Best Practice" stated that the critical success factor of the ERM is the result of proper identification and risk grouping. This research used primary data obtained through interview and questionnaire filling. The result of this research is about the application of ERM, in theory, the practice of which has not been applied to Industry.

(Osunmuyiwa, 2013) in his research on "Online Banking and The Risk Involved" reviewed the implementation of online banking services that will provide the customers with the convenience and flexibility in accessing banking services via the Internet at home or elsewhere without having to come to the bank. In addition to these ease and flexibility factors, there are potential risks that arise in connection with this online banking application including strategic risk,

transaction risk, compliance risk, reputation risk, and information security risk.

(Sarma & Singh, 2010) in his journal about "Risk Analysis and Applicability of Biometric Technology for Authentication", one of the ways to mitigate risks is to apply security access using biometric authentication such as fingerprint detection, face, voice, body movement, and others. This study discusses how risk mitigation uses biometrics without using the ERM.

(Bahl, 2012) in his paper on "E-Banking: Challenges and Policy Implication" review the implementation of e-banking as a new opportunity for the banking industry. Although some countries have successfully implemented e-banking, to further refine the implementation of e-banking macroeconomic policy is required to determine the terms of cost and sustainability. Table 1 presents some of the previous research that has been done regarding the implementation of online banking and ERM.

Table 1.
Previous Research Related to Online Banking and ERM

Title	Authors	Methods	Results
Integration of Risk Management into Strategic Planning: A New Comprehensive Approach	Isabela Ribeiro Damaso Maia & George Montgomery Machado Chaves (2016)	SWOT and ERM	The research was conducted in public company where the obtained result was the biggest risk caused by strategic risk. The company failed to integrate risk management to company strategies.
Integrated Enterprise Risk Management: From Process to Best Practice	Kathryn Cormican (2014)	ERM	The critical success factors of the ERM are the results of risk identification and grouping.
Risk Mapping in the Tannery Industry with ERM Approach	Helen Wiryani, Noer Azam Achsani, Lukman M. Baga (2013)	ERM	The strategy that needs to be developed for effective risk mitigation for PT XYZ is to prioritize the handling of the highest risk first and then to lower risk.
Implementation of Enterprise Risk Management in order to Improve the Effectiveness of Operational Activities of CV *Anugerah Berkat Calindojaya*	Mellisa and Fidelis Arastyo Andono (2013)	ERM	The ERM implementation helps CV.ABC in finding risks at high, medium, and low levels. Risks that are classified as high risk are risks that must be considered by management and should be handled as soon as possible. The risk classified as medium risk has not a significant impact on the company. The risk that is classified as low risk is a risk that comes after the medium and high risks.
Report on The Current State of Enterprise Risk Oversight	Mark Beasley, Bruce Branson, Bonnie Hancock (2015)	ERM	There are still many companies that have not carefully taken care of risks, especially those related to strategies. The need to evaluate the process of risk management is based on the volume and complexity and the events experienced by the company

Table 1.
Previous Research Related to Online Banking and ERM - Continued

Title	Authors	Methods	Results
Online Banking and The Risk Involved	Lufolabi Osunmuyiwa (2013)	Literature review	The potential risks that arise in connection with the implementation of this online banking include risks such as strategic risk, transaction risk, compliance risk, reputation risk, and information security risk.
Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication	Gunajit Sarma and Pranav Kumar Singh (2010)	Literature review	One way to mitigate security risks related to online banking system access is through the application of security access using biometric authentication such as fingerprint detection, face, voice, body movement, and others.
Internet Banking, Security Models, and Weakness	Bilal Ahmad Sheikh and Dr. P. Rajmohan (2015)	Literature review	Access security model of the internet banking that is currently widely used is based on user identification and authentication methods. However, if the Bank does not mitigate the risk of data loss and access security, it will result in fraud. The new solution to strengthen the access security is using biometric authentication
The Role and Importance of Risk Management In Internet Banking	Mojtaba Mali, Hossein Niavand, and Farzaneh Haghighat Nia (2014)	ERM	The most vulnerable risk is security risk related to transaction security, customer data security, and user access security. These risks need to be identified, classified, and risk assessments involving management in banks that have the competence to determine potential risks
E-Banking: Challenges and Policy Implication	Dr. Sarita Bahl (2012)		The implementation of e-banking as a new opportunity in the banking industry. Although some countries have successfully implemented e-banking, to further refine the implementation of e-banking, macroeconomic policy is required to determine the terms of cost and sustainability

III. METHODOLOGY

The types of data used in this study are primary and secondary data. The collected primary data were obtained from interviews and questionnaires, while secondary data were obtained through the publication of annual reports, financial reports, and other sources related to this research. The implementation of this research was conducted at Bank XYZ Head Office as an object that has implemented online banking.

Sampling for primary data was done with a specific purpose (purposive sampling) i.e. the sample taken with the purpose and certain considerations addressed to the respondents who will be interviewed in depth. The respondents, in this study, are internal Bank XYZ who have competency, capacity, and experience in the field of operational and risk management processes including risk management division, operational division, and business division. Each division provided as much as two respondents at the managerial level and two respondents at the head of unit level. Thus, a total of respondents 12 respondents was used. The respondents were selected to represent their respective divisions and directly involved in the creation of operational processes and online banking risk assessment process at Bank XYZ.

Research stages started from the data collection through the questionnaire filling which was done by conducting in-depth interviews to obtain information about the potential risks and risk mitigation that will be done. This research was conducted by using the descriptive approach in the form of the case study which was a detailed study (and in-depth related) of the object to be studied. Risk research carried out through the ERM (Enterprise Risk Management) method adapts to the ERM framework for obtaining risk mapping of the implementation of online banking.

IV. RESULTS AND ANALYSIS

The online banking risk mapping, at Bank XYZ, was conducted using the ERM framework. The stages of the implementation in this research were conducted by referring to the eight components of ERM, namely internal environment, objective setting, event identification, risk assessment, risk response, control, information, and communication, monitoring.

4.1. ERM 1*:* Internal Environment

The implementation of online banking services, at Bank XYZ, is done by focusing on serving the smartphone user segment. This is in line with the company's goal of improving service to customer oriented and utilizing digital technology. Bank XYZ's governance is implemented by applying Good Corporate Governance (GCG) which is to identify and control risk to improve the existing business process and apply the four eyes principles in which every process is done by dual control. Every business process, that is executed, must have standardized rules set forth in the form of policies or procedures and set its periodic evaluation plan.

4.2. ERM 2*:* Objective Setting

The objective setting of Bank XYZ can be seen from the four priority sides based on the ERM framework which includes Strategic Objective, Operating Objective, Reporting Objective, and Compliance Objective. In the strategic objective, XYZ Bank took the initiative to innovate in finance by developing online banking business that utilizes smartphone media to be able to provide financial and non-financial transactions to the community. In the operating objective, Bank

XYZ continuously improves the Bank's operational processes to enhance the effectiveness and efficiency of work processes and costs, in addition to conducting periodic evaluations of work processes that have been previously applied. In the reporting objective provides transparent and accurate reports for both internal and external parties. This is necessary so that the company can take appropriate steps for decision making and as accountability to stakeholders. The compliance objective complies with the regulations set by the government and regulator (BI and OJK) as well as the rules applicable regionally and internationally to be in line with the established Bank Business Plan.

4.3. ERM 3: Event Identification

The risk identification process of the online banking application at Bank XYZ is based on the deposition of risk categories based on BI and OJK rules covering credit risk, market risk, operational risk, liquidity risk, compliance risk, legal risk, reputation risk, and strategic risk. The risk identification process is conducted through in-depth interviews with those who have competencies in the areas of risk and operational processes. Based on the results of the identification, 55 potential risks from the implementation of online banking at Bank XYZ were observed. Table 2 presents potential risk obtained based on the identification results.

Table 2.
Risk Identification Results

Risk Categories	Risks No	Risks Identification
Liquidity risks	R1	Banks are bankrupt and customer funds are non-refundable
	R2	The customer keeps funds in small amount and short term, so the Bank does not get big fund in the long-term
Credit risks	R3	The Customer feeling the obligation to pay the loan to the Bank is reduced because it is not directly related to the Bank
	R4	The Customer does not make any loan payments to the Bank
	R5	Bank does not conduct customer analysis for customer who applies for loan
	R6	The Bank can not provide customer loan data or information for reporting
	R7	Lack of transparency on loan product information to customers leading to customer complaints
	R8	A change of policy from the government or regulator related to credit regulations
Market risks	R9	Changes in the value of the Rupiah (currency)
	R10	Changes in interest rates

https://bulletin.bmeb-bi.org/bmeb/vol20/iss3/5
DOI: 10.21098/bemp.v20i3.824

Table 2.
Risk Identification Results - Continued

Risk Categories	Risks No	Risks Identification
Strategic risks	R11	Fail to achieve product sales target
	R12	Fail to develop products according to customers' needs
	R13	Fail to acquire new customers
	R14	Fail in prioritizing strategy
	R15	Competitors get a large market share
	R16	The Bank's fails to build an integrated network system with partners
	R17	Top management that has the capability to provide strategic direction, withdraw from the company
	R18	Partner work is not in line with agreement
Operational risks	R19	Customer can not transact due to forgotten PIN or User ID
	R20	The absence of clear procedures and business processes
	R21	The controlling process of the activity that has been executed does not exist yet
	R22	The password or PIN length is very complicated
	R23	Customer fails to make transactions via ATM
	R24	Less effective process
	R25	Error doing data input caused by lack of information on the input procedure
	R26	The political situation that leads to riots or demonstrations
	R27	Natural disasters on a national scale
	R28	Theft of Bank information by Customer/Internal Party/External Parties
	R29	The customer can not access the transaction through online banking due to the absence of the network or trouble with the system provider (down)
	R30	Bank systems are vulnerable to viruses or malware
	R31	SMS or Email delivery as transaction proof failed to be sent
	R32	Failure to store customer data and back it up
	R33	Theft of customer user ID by external parties
	R34	The fraud perpetrator acts on behalf of the client and unlawfully accesses the customer's account
	R35	Fraud actor that acts on behalf of the Bank and requests User ID or Password of the customer for fraud

Table 2.
Risk Identification Results - Continued

Risk Categories	Risks No	Risks Identification
	R36	Fraud perpetrators work with Bank employees to link ATMs with personal account numbers or other accounts
	R37	Fraud perpetrators use other domains to access the Bank system
	R38	The Customer denies transactions that have been made
	R39	The Customer has made an initial deposit for opening an account, but the account opening is rejected by the Bank
	R40	The Bank system is hijacked by external parties
	R41	Employees open fake accounts with customers to get incentives
	R42	The Customer can not provide identity cards and other mandatory documents
	R43	Customers do not receive ATM cards
	R44	The Bank does not have backup for Customer data
Reputation Risks	R45	Fraud is detrimental to customers
	R46	Failed transaction
	R47	Customer's location of the transaction does not receive signal
	R48	Customer complaints services are long
	R49	Employees of the Bank require remuneration to the Customer for the services provided
Compliance Risks	R50	The Bank does not fulfill the data fulfillment obligation for KYC Customer
	R51	Rule changes from the regulator
	R52	Rules of BI and/or OJK that cannot be fulfilled by the Bank
Legal risks	R53	The Bank cannot resolve the dispute with the Customer
	R54	Lack of clauses in the agreement made by the Bank with the Customer
	R55	Changes in laws and regulations that cause the Bank to change all or part of its agreement with the customer

Source: Processed Data of Bank XYZ (2016)

4.4. ERM 4: Risk Assessment

The next stage of risk identification is risk assessment based on probability and impact. The categorization of risks based on probability is divided into five scales i.e. very low, low, medium, high, and very high (Godfrey, 1996). The impact scale indicator refers to the criteria of risk probability indicators established by internal Bank XYZ. The indicators are obtained based on historical data of events within a period of one year (2016-2017) i.e. based on data of customer's complaints audit and internal complaints of bank related to system or IT. Table 3 represents risk indicators based on probability.

Table 3.
Risk Indicators based on Probability

No	Categories	Guidelines	Scale
1	Very low (improbable)	≤ 10 incidences per year	1
2	Low (remote)	11 – ≤ 20 incidences per year	2
3	Medium (occasional)	21 – ≤ 30 incidences per year	3
4	High (probable)	31 – ≤ 40 incidences per year	4
5	Very high (frequent)	> 41 incidences per year	5

Source: Processed Data of Bank XYZ (2016)

The classification of risk categories based on impact is divided into five scales: neglected, small, medium, large, and very large (Godfrey, 1996). The risk impact indicators used are sourced from the criteria indicated by Bank XYZ that are financial, regulatory, reputation, legal, and information security impacts. Each of these guidelines has its own risk impact weight in accordance with acceptable risk acceptance by Bank XYZ. Table 4 presents an impact-based risk indicator.

Table 4.
Risk Indicator based on Impacts

No	Categories	Guidelines					Scale
		Financial	Regulatory	Reputation	Legal	Information security	
1	Negligible	Profit is reduced < 10%	There is no reprimand from the regulator	• No complaints in local/ national media	• There are no mistakes in the agreement clause	• Classification of internal data/ information	1
				• Customer complaints increased by 10%	• There is no violation of the law • There is no claim from the Customer	• Data leak/ information that does not provide benefits to internal parties	
2	Marginal	Profit is reduced 10 % - ≤ 20%	There is a verbal reprimand from the regulator	• Submission of complaints to at least one Local/ national media • Customer complaints increased from 10.1% - 20%	• The existence of deficiencies in the agreement clause (minor) • There is no violation of the law • There is no claim from the Customer	• Classification Internal data/ information • Data leak/ information that provides benefits to internal parties	2

Table 4.
Risk Indicator based on Impacts - Continued

No	Categories	Guidelines					Scale
		Financial	Regulatory	Reputation	Legal	Information security	
3	Serious	Profit is reduced 20% - ≤ 30%	• There is a written reprimand from the regulator • No penalties	• Submission of complaints to at least two local/national Media • Customer complaints increased from 20.1% - 30%	• The existence of an error in the agreement clause (minor) • There is no violation of the law • There is no claim from the Customer	• Classification of internal data/ information • Leakage of data/ information that does not provide benefits to external parties	3
4	Critical	Profit is reduced 30% - ≤ 40%	• There is at least one written reprimand from the regulator • There are penalties	• Submission of complaints to at least two Local/ national medias • Customer complaints increased from 30.1% to 40%	• The existence of an error in the agreement clause (major) • There is no violation of the law • There is no claim from the Customer	• Classification of internal data/ information • Data leak/ information that provides benefits to external parties	4
5	Catastrophic	Profit is reduced > 40%	• There are written reprimands from the regulator >1 • There are penalties	• Submission of complaints to at least 3 local / national medias • Customer complaints increased> 40%	• The existence of a violation of the law • The existence of a claim from the Customer	• Classification of confidential data/ information • Data leak/ information that provides benefits to internal and/or external parties	5

Source : Bank XYZ processed Data (2016)

Having determined the risk indicators based on both the probability and impact, the next step is scoring which is carried out to determine the risk level of each identified potential risk. The level of risk is divided into five categories of risk level as follows: High (H), Medium to High (MH), Medium (M), Low to Medium (LM), and Low (L). Table 5 presents the result of risk scoring of each identified potential risk.

Table 5.
Risk Scoring Results

Risk Categories	No	Risk Identification	Score P	Score D	Total Score (P x D)	Risk Levels
Liquidity Risks	R1	Banks are bankrupt and customer funds are non-refundable	1	5	5	MH
	R2	The customer keeps funds in small amount and short term, so the Bank does not get big fund in the long-term	5	2	10	M
Credit Risks	R3	The Customer feeling the obligation to pay the loan to the Bank is reduced because it is not directly related to the Bank	3	2	6	M
	R4	The Customer does not make any loan payments to the Bank	5	5	25	H
	R5	Bank does not conduct customer analysis for customer who applies for loan	3	4	12	H
	R6	The Bank can not provide customer loan data or information for reporting	1	4	4	MH
	R7	Lack of transparency of loan product information to customers, leading to customer complaints	2	5	10	MH
	R8	Policy changes from government or regulators regarding credit regulations	1	4	4	MH
Market Risks	R9	Changes in the value of the Rupiah (currency)	3	1	3	LM
	R10	Changes in interest rates	1	2	2	LM
Strategic Risks	R11	Fail to achieve product sales target	2	4	8	MH
	R12	Fail to develop products according to customers' needs	1	4	4	MH
	R13	Fail to acquire new customers	5	4	20	H
	R14	Fail in prioritizing strategies	1	4	4	MH
	R15	Competitors get a large market share	3	4	12	H
	R16	The Bank fails to build an integrated network system with partners	1	2	2	LM
	R17	Top management, that has the capability to provide strategic direction, withdraw from the company	1	1	1	L

Table 5.
Risk Scoring Results - Continued

Risk Categories	No	Risk Identification	Score P	Score D	Total Score (P x D)	Risk Levels
	R18	Partner work is not in line with the agreement	1	5	5	MH
	R19	Customer can not transact due to forgotten PIN or User ID	5	2	10	M
Operational Risks	R20	The absence of clear procedures and business processes	1	3	3	M
	R21	The controlling process of the activities that have been executed does not exist yet	1	5	5	MH
	R22	The password or PIN length is very complicated	3	1	3	LM
	R23	Customer fails to make transactions via ATM	2	2	4	LM
	R24	Less effective process	1	5	5	MH
	R25	Errors during data input caused by lack of information procedure input	1	3	3	M
	R26	The political situation that leads to riots or demonstrations	1	1	1	L
	R27	Natural disasters on a national scale	1	4	4	MH
	R28	Theft of Bank information by Customer / Internal Party / External Parties	1	5	5	MH
	R29	The customer can not access the transactions through online banking due to the absence of the network or trouble with the system provider (down)	5	2	10	M
	R30	Bank systems are vulnerable to viruses or malware	1	4	4	MH
	R31	SMS or Email delivery as transaction proof failed to be sent	3	1	3	LM
	R32	Fail to store customer data and back it up	1	5	5	MH
	R33	Theft of customer user ID by external parties	1	5	5	MH
	R34	The fraud perpetrator acts on behalf of the client and unlawfully accesses the customer's account	1	5	5	MH

Table 5.
Risk Scoring Results - Continued

Risk Categories	No	Risk Identification	Score P	Score D	Total Score (P x D)	Risk Levels
	R35	Fraud perpetrator acts on behalf of the Bank and requests User ID or Password of the customer for fraud	2	5	10	MH
	R36	Fraud perpetrators work with Bank employees to link ATMs with personal account numbers or other accounts	2	5	10	MH
	R37	Fraud perpetrators use other domains to access the Bank system	1	5	5	MH
	R38	The Customer denies transactions that have been made	1	5	5	MH
	R39	The Customer has made an initial deposit for opening an account, but the account opening is rejected by the Bank	1	4	4	MH
	R40	The Bank system is hijacked by external parties	1	5	5	MH
	R41	Employees open fake accounts with customers to get incentives	1	5	5	MH
	R42	The Customer can not provide identity cards and other mandatory documents	5	1	5	M
	R43	Customers do not receive ATM cards	5	3	15	MH
	R44	The Bank does not have backup for Customer data	1	5	5	MH
	R45	Fraud is detrimental to customers	2	5	10	MH
	R46	Failed transaction	4	3	12	MH
	R47	Customer's location of the transaction does not receive signal	4	3	12	MH
	R48	Customer complaints services are long	3	5	15	H
	R49	Employees of the Bank require remuneration to the Customer for the services provided	2	3	6	M
Compliance Risks	R50	The Bank does not fulfill the data fulfillment obligation for KYC Customer	1	4	4	MH
	R51	Rule changes from the regulator	1	4	4	MH
	R52	Rules of BI and/or OJK that cannot be fulfilled by the Bank	1	4	4	MH

Table 5.
Risk Scoring Results - Continued

Risk Categories	No	Risk Identification	Score P	Score D	Total Score (P x D)	Risk Levels
Legal Risks	R53	The Bank cannot resolve the dispute with the Customer	1	5	5	MH
	R54	Lack of clauses in the agreement made by the Bank with the Customer	1	4	4	MH
	R55	Changes in the laws and regulations that cause the Bank to change all or part of its agreement with the customer	1	5	5	MH

Source: Bank XYZ processed Data (2016)

Once the risk score results are obtained, we can proceed to make the risk map according to the five risk levels. To make the differentiation easier, the five levels of risk were divided into several colors: High (H) red, Medium to High (MH) orange, Medium (M) yellow, Low to Medium (LM) dark green, and Low (L) green. Figure 1 represents the results of the risk mapping that has been done.

Figure 1. Results of Risk Mapping prior to Mitigation

	Negligble (1)	Marginal (2)	Serious (3)	Critical (4)	Catastrophic (5)
Frequent (5)	R42	R2, R19, R29	R43	R13	R4
Probable (4)			R46, R47		
Occasional (3)	R9, R22, R31	R3		R5, R15	R48
Remote (2)		R23	R49	R11	R7, R35, R36, R45
Improbable (1)	R17, R26	R10, R16	R20, R25	R6, R8, R12, R14, R27, R30, R39, R50, R51, R52, R54	R1, R18, R21, R24, R28, R32, R33, R34, R37, R38, R40, R41, R44, R53, R55

Source: Processed data of Bank XYZ (2016)

4.5. ERM 5: Risk Response

Based on the results of the risk mapping that has been done, the risk mitigation measure can be carried out. The identified potential risks are risk mitigation measures so that each risk can be monitored and not shifted towards a higher

level of risk. The main priority of the risk mitigation starts with the High-risk level, followed by level Medium to High, Medium, Low to Medium, and finally low-risk level. The risk response to the identified risks, at Bank XYZ, is shown in Table 6.

Table 6.
Risk Response to the Identified Risks

Risk Category	Identified Risks	Risk Responses
Liquidity Risks	Banks are bankrupt and customer funds are non-refundable	1. Apply the rules set by BI and OJK, in particular, the implementation of risk management for liquidity risk. 2. Socialize with the customer on the fact that the Bank's fund is guaranteed by LPS with a maximum amount of 2 Billion Rupiah per customer.
	The customer keeps funds in small amount and short term, so the Bank does not get big fund in the long-term	1. Reward the customers who make deposits in certain nominal and a certain period of time. 2. Provide interest rates above the average of the competitors.
Credit Risks	The Customer feeling the obligation to pay the loan to the Bank is reduced because it is not directly related to the Bank	1. The Bank shall be required the verification of the customer upon the submission of the loan through a visit to the customer, by telephone, or other media in accordance with BI and/or OJK rules related to KYC (know your customer). 2. Mandatory credit agreement on approved loan. Credit agreements may be sent by mail or email.
	The Customer does not make loan payments to the Bank	The Bank sets out the Client's criteria to be granted such as: 1. Customer's balance for 6 consecutive months amounts to Rp. 500,000 and above. 2. Make transactions through online banking each month, at least 5 times. 3. Establish the criteria for customer's job that is eligible for a loan.
	Bank does not conduct customer analysis for customer who applies for loan	1. Banks are required to establish rules or policies regarding credit processes that include credit required documents, credit application process, data verification, credit limit, credit approval until the control process must be performed.

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
		2. Banks can collaborate with third parties to conduct credit score analysis process of the customers applying for loans.
	The Bank can not provide customer loan data/information for reporting	1. Fulfill all customer information required under SID rules (debtor information system) in online banking system 2. Storage is required on server or cloud to store customer's data as the whole process is done online. 3. Set the retention period for customer data storage.
	Lack of transparency of loan product information to customers, leading to customer complaints	1. The Bank provides a special menu on the online banking display that contains product information in the form of product specifications, costs, and the risks attached to the product. 2. The existence of disclaimer-specific pages prior to the submission of credit sent by the customer containing information that the customer has been given explanation and understand the product he selected. 3. Banks are required to submit credit agreements on loans approved by letter or email from customers.
	There is a change of policy from the government/regulator related to credit regulations.	1. The compliance working unit monitors every published government, BI and/or OJK. regulations and reviews the rules 2. Coordinate with work units related to changes in rules such as business, operational, IT, and other units for action.
Market Risks	Changes in the value of Rupiah (currency)	1. The risk of changes in the value of Rupiah can be ignored because the current online banking implementation uses the Rupiah as currency.
	Changes in interest rates	1. Inform the Customer of interest rate changes through email, SMS, or other media.

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
Strategic Risks	Fail to achieve product sales target	1. Determine realistic product sales target according to target market segment. 2. Create tools that contain information on the achievement of sales targets for each sale as material evaluation of target achievement.
	Fail to develop products according to customers' needs	1. Analyze the market to determine which market segments to target by utilizing market analytic divisions or using consultant services.
	Fail to acquire new customers	1. Conduct promotion through various media, especially social media. 2. Provide promotion by cooperating with store/merchant to offer discount on the purchase certain product.
	Fail in prioritizing strategies	1. Set realistic target priorities to be achieved as directed by management. Target priority is submitted along with the timeline/ date of its realization.
	Competitors get a large market share	1. Provide customer services such as free transaction fee for 50 transactions every month. 2. Offer interest rates above the average of the competitors.
	The Bank fails to build an integrated network system with partners	1. Provides 2 network models namely online mode and offline mode. So if the online mode of the system is not running, it will be transferred automatically to offline mode.
	Top management that has the capability to provide strategic direction, withdraw from the company	1. Divide the tasks and responsibilities to some senior management. In addition to providing training to employees who are considered to have good potential.
	Partner work is not in line with the agreement	1. Make a cooperation agreement (MCC) that contains agreement on the responsibility of both parties, the completion of work, including the steps that must be taken in case of default.

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
Operational Risks	Customer can not transact due to forgotten PIN or User ID	1. Provide the User ID/Password forgot feature on the online banking application and connect it to the email/mobile phone number of the Customer.
	The absence of clear procedures and business processes	1. The working units, connected to the online banking process, work together to coordinate the formulation of policies or procedures to develop the operational processes and control those to be run.
	The controlling Process of the activities, that have been executed, does not yet exist	1. Standardize rules in the form of Policies or SOPs which contains operational processes that run along with the control process that must be carried out.
	Password length/PIN is very complicated	1. Provide PIN / Password reset feature in the online banking application connected with customer's email/phone number. 2. Use biometric authentication in the form of fingerprint scanning or face recognition.
	Customer fails to make transactions via ATM	1. Make transaction features, via smartphone, as a key feature in online banking services.
	Less effective process	1. Evaluate the process that has been implemented by involving various related units so that more objective input and suggestions can be obtained.
	Error in the input data caused by lack of information in the input procedure	1. Create an input procedure that is poured in the form of user manual document. 2. Specify mandatory fields in accordance with BI and/or OJK requirements to be adjusted in the online banking system.
	Political situation that leads to riot/ demonstration	1. Make transaction features via smartphone as a key feature in online banking services.
	Natural disasters on a national scale	1. Make transaction features via smartphone as a key feature in online banking services.

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
		2. The security of server/IT devices/ network systems supporting the online banking implementation must be carried out through the Business Continuity Plan (BCP) to keep business processes running.
	Theft of Bank information by Customer / Internal Party / External Parties	1. Classify the data into 3 categories which are general, internal, and secret. 2. Restrictions on access to information according to classification based on positions and working units. 3. Standardization of the documents or files naming according to classification. 4. Encrypt if documents or files are sent via email.
	The customer can not access the transaction through online banking due to the absence of the network or trouble with the system provider (down)	1. Working with providers with a wide internet network. 2. Provides information to the Customer through display on the Customer's smartphone in relation to the constraints that are being experienced, and directing the Customer to transact through other channels such as ATM.
	Bank systems are vulnerable to viruses or malware	1. Periodically update antivirus and firewall. 2. Restrict access to certain web via internet. 3. Restrict access to USB usage on a computer or laptop device.
	SMS/Email delivery as transaction proof fails to send	1. Provide proof of transaction notification in online banking feature in the form of transaction history information for the customer.
	Fail to store customer data and back it up	1. The need for storage or special storage in the server or cloud to store Customer data in connection with all customer input data carried out online. 2. Set a retention period for customer data storage.

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
	Theft of customer user ID by external parties	1. Include information related to the confidentiality of User ID and password at the end of the online banking display when opening an account. 2. Set a password change so that the Customer has to change the password every 3 months. 3. Perform a periodical reminder via SMS or email to the Customer on the need to maintain the confidentiality of the User ID and password.
	The fraud perpetrator acts on behalf of the client and unlawfully accesses the customer's account	1. Submitting the authentication code to the Customer's mobile phone for any transactions done by the Customer as a means of verifying the validity of the transaction.
	The fraud perpetrator acts on behalf of the Bank and asks the User ID/Password of the customer for fraud	1. Perform a periodical reminder via SMS or email to the Customer on the need to maintain the confidentiality of the User ID and password. 2. Provide harsh sanctions to employees who are proven of committing fraud.
	Fraud perpetrators work with Bank employees to link ATMs with personal account numbers or other accounts	1. Apply dual control process (checker and maker) on the linking ATM number process with Customer's account. 2. Provide harsh sanctions to employees who are proven of committing fraud.
	Fraud perpetrators use other domains to access the Bank system	1. Restricting system access using only the Bank's internal domains.
	The Customer denies transactions that have been made	1. Send the authentication code to the Customer's mobile phone for any transactions done by the Customer as a means of verifying the validity of the transaction. 2. The delivery of transaction evidence by email or SMS.
	The Customer has made an initial deposit for opening an account, but the account opening is rejected by the Bank	1. Information is provided that the account opening process, made by the Customer, is semi-active and the Customer will be able to use the account on a regular basis after obtaining approval from the Bank.

https://bulletin.bmeb-bi.org/bmeb/vol20/iss3/5
DOI: 10.21098/bemp.v20i3.824

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
		2. Require the inclusion of column of account number of destination account for refund in case of account opening decline. 3. Rules are made regarding refund of customer's funds and their returning SLA to the Customer.
	The Bank system is hijacked by external parties	1. The IT Security working unit is required to monitor all system and network security used by the Bank such as performing the vulnerability assessment. Such monitoring shall be conducted periodically.
	Employees open fake accounts with customers to get incentives	1. The Bank is required to verify to the Customer upon opening of the proposed account through a visit to the Customer, by telephone, or other media in accordance with BI and/or OJK rules related to KYC (know your customer). 2. Create a direct integration between the Bank system and the Dukcapil system (Population and Civil Registry) to verify the customer data.
	The Customer can not provide identity cards and other mandatory documents	1. Create a mandatory document field for the customer so that account opening cannot be processed further if the document is not provided.
	Customers do not receive ATM cards	1. Make a notification to the system that the customer has not received yet the ATM card for H + 2 since the opening of Customer's account was approved by Bank.
	The Bank does not have backup for Customer data	1. A special storage for customer data back up is required in the server or cloud separated from the core storage.
Reputational Risks	Fraud that is detrimental to customers	1. Provide harsh sanctions to employees who are proven of committing fraud. 2. Socialize all employees regarding the actions of fraud and sanctions.

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
	Failed transaction	1. Work with providers that have a wide internet network. 2. Ensure that the infrastructure that supports online banking services runs well. 3. Compulsory rules must be made when receiving complaints from the Customer, such as the Customer is directed to transact through ATM.
	Customer's location of the transaction does not receive signal	1. Work with providers that have a wide internet network. 2. ATM Provides information to the Customer through display on the Customer's smartphone in relation to the constraints that are being experienced, and direct the Customer to transact through other channels such as ATM.
	Customer complaints services are long	1. Create a special unit that handles customer complaints. 2. Establish the SLA and inform the customer. 3. Inform the Customer that the complaint service can be reached through the contact center.
	Employees of the Bank require remuneration to the Customer for the services provided	1. Provide an appeal to the Client not to provide any kind of compensation to Bank officers through email or SMS media. 2. Provide strict sanctions to Bank officers who are proven to require remuneration from the Customer.
Compliance Risks	The Bank does not accomplish the data fulfillment obligation for KYC Customer	1. Ensure that the Bank's system meets all Customer's required information according to KYC (know your customer) rules at the time of account opening. 2. The KYC process is recommended to be performed by a third party with due regard to the rules of BI and/or OJK. 3. The Compliance Work Unit has reviewed the KYC scheme by third parties. 4. Socialization related to KYC process conducted by the third party.

https://bulletin.bmeb-bi.org/bmeb/vol20/iss3/5
DOI: 10.21098/bemp.v20i3.824

Table 6.
Risk Response to the Identified Risks - Continued

Risk Category	Identified Risks	Risk Responses
	Rule changes from the regulator	1. The Compliance Work Unit monitors every published government, BI and/or OJK regulations and reviews the rules. 2. Coordinate with work units related to changes in rules such as business, operational, IT, and other units for action.
	Rules of BI and/or OJK that cannot be fulfilled by the Bank	1. The Compliance Work Unit reviews the rules of BI and/ or OJK and coordinates with relevant work units regarding business process readiness, system readiness, rule readiness, and other infrastructure required to comply with these rules.
Legal Risks	The Bank cannot resolve the dispute with the Customer	1. List all of the terms of the relationship between the Bank and the Client including the procedure of settlement in the event of a dispute. All of which are contained in clauses/agreements and approved by the Customer at the opening of online banking.
	Lack of clauses in the agreement made by the Bank with the Customer	1. The Legal Work Unit is obliged to review the entire clause of the agreement and ensure all aspects of the agreement have been met.
	Changes in laws and regulations that cause the Bank to change all or part of its agreement with the customer	1. The Legal Work Unit monitors every change in published legislation and reviews the rules. 2. Coordinate with work units in relation to changes in rules such as business, operational, IT, and other units for action.

Source: Bank XYZ processed Data (2016)

After the risk mitigation, the process continues with the risk mapping stage which is carried out to obtain an overview of the residual risk. This stage is done through the distribution of questionnaires and in-depth interviews with the parties with competencies in the field of risk and operational processes. The purpose of doing the risk mapping, after mitigation, is to obtain a picture of changes in the risks that occur when the mitigation actions are executed. The risk map, after the risk mitigation process at Bank XYZ, is shown in Figure 2.

Figure 2. Results of Risk Mapping Post Mitigation

	Negligble (1)	Marginal (2)	Serious (3)	Critical (4)	Catastrophic (5)
Frequent (5)	R2, R42	R19, R29, R43	R13, R4		
Probable (4)		R46, R47	R5, R15		
Occasional (3)	R3, R22, R31				
Remote (2)	R9, R23	R49	R11	R7, R35, R36, R45	R48
Improbable (1)	R17, R26, R10, R16	R20	R6, R8, R12, R14, R25, R27, R30, R32, R33, R34, R37	R1, R18, R21, R24, R28, R38, R39, R50, R51, R52, R54	R40, R41, R44, R53, R55

Sumber: Data Bank XYZ (2016) diolah

Based on the results of risk mapping, after mitigation, it can be seen that there are five potential risks, that previously included the High-risk level, have turned into Medium to High-risk level. However, there are also potential risks that have been mitigated but remain at the same level of risk as before, such as the risk of partner or third party work not in accordance with the agreement. Based on the results of the discussions with respondents, this is due to various factors such as the condition of the partner company experiencing the problem, or the person responsible in the process of withdrawing from the company who took the risk despite mitigation but the risk level has not changed. This level of risk is mandatory for periodic monitoring so that the risk level does not move into higher risk levels.

4.6. ERM 6: Control Activities

Control measures are taken to minimize losses incurred by risk and ensure the effectiveness of the responses to risk. Control can be done by Bank XYZ by giving a clear job description for each employee covering specific responsibilities and authorities in the work. The strict monitoring of the implementation of procedures or policies through periodic inspections by the Internal Audit working unit covering all processes should be undertaken along with periodic evaluations of all performance executed in order to address issues or problems arising from the process undertaken which become an important part of the control process.

4.7. ERM 7: Information and Communication

The results of the risk assessment that have been undertaken and the risk mitigation advice that has been given must be transmitted and socialized to each related work unit both internal or external to the company, and third-party that is related

to activities to be followed up so that the potential risk can be controlled. The transmission to the related parties can be in the form of a document procedure or policy or a Cooperation Agreement. In addition, the selection of the communication methods is also important to ensure that the information is delivered. Internal communication methods can be internal meetings using meeting minutes, special portals commonly accessed by employees email. The method of information transmission should also be easy to understand and adequately explained so that each employee understands the information submitted.

4.8. ERM 8: Monitoring

All identified risks must be periodically monitored to keep the risks under control. The supervision can be done through the monitoring of ongoing activities or processes or performing separate evaluations or a combination of both. In addition, there is a need to hold the regular internal meeting to discuss issues or problems arising from the process undertaken. In conducting the monitoring activities, each working unit associated with the process, Internal Audit, along with Risk Management, conducts assessments of various risks, monitors operational activities, and reports the evaluation results to the senior management.

V. CONCLUSIONS

The potential risks identified in the implementation of online banking services are reviewed through eight risk categories established by BI and OJK among as many as 55 potential risks. Strategies applied for effective risk mitigation are more often done for mitigating identified risks. This is done because the online banking business is in the process of development, so the Bank is optimistic about the prospect of online banking business which should still be guided by the rules that apply.

The results of this study are intended to guide in minimizing the emergence of risks through periodic risk control that involves working units related to the online banking process. Furthermore, monitoring, based on the results of customer complaints data and the internal audit of the process undertaken, can be used as the basis for improvement and evaluation in order to monitor other risks that may emerge in the process and were not previously identified.

Implications for the Bank, in connection with the implementation of online banking, in terms of strategic areas i.e. all the company's strategy to be achieved must be included in a written documents or presentations and socialized to all employees. The operational areas of continuous improvement must be performed through suggestions for innovative and creative process improvement in order to achieve company goals. The reporting field should provide back up data for reporting in relation to some previously unavailable data. Perform data storage or customer information and transaction documents in digital form according to regulatory provisions and retention period of storage. The areas of compliance make sourced policy or procedure in accordance with the applicable law and regulatory regulations. In addition, standardizing the control process for each policy or procedure undertaken with the objective of minimizing the risk posed.

REFERENCES

Bahl, S. (2012). E-Banking: Challenges & Policy Implications. *Proceedings of "I-Society 2012" at GKU*, 1–12.

Baldwin, A., Shiu, S. (2010). Managing Digital Risk Trends, Issues, and Implications for Business. (n.d.).

Bank Indonesia. (2016). Financial Technology (FinTech) "Analisa Peluang Indonesia dalam Era Ekonomi Digital dari Aspek Infrastruktur, Teknologi, SDM, dan Regulasi Penyelenggara dan Pendukung Jasa Sistem Pembayaran. *Temu Ilmiah Nasional Peneliti 2016 – Kemenkominfo*, 1–31

Godfrey. (1996). Control of Risk a Guide to The Systematic Management of Risk from Construction1.pdf. (n.d.).

Cormican, K. (2014). Integrated Enterprise Risk Management : From Process to Best Practice. *Modern Economy*, (April), 401–413.

COSO-ERM. (2004). Enterprise Risk Management — Integrated Framework, *3*(September), 1–16. https://doi.org/10.1504/IJISM.2007.013372

Darmawi. (2006). Manajemen Risiko. Edisi ke-10. Jakarta : Bumi Aksara.

Djohanputro, B. (2008). Manajemen Risiko Korporat. Pendidikan dan Pembinaan Manajemen. Jakarta.

Diversitas, K. I. (2008). Tinjauan pustaka, 5–20.

Eistert, T., Deighton, J., Marcu, S., Gordon, F., & Ullrich, M. (2013). Banking in a Digital World. *AT Kearney*, 23. Retrieved from http://www.atkearney.de/financial-institutions/ideas-insights/featured-article/ /asset_publisher/4rTTGHNzeaaK/content/banking-in-a-digital-world

Ndlovu, I., & Sigola, M. (2013). Benefits and Risks of E-Banking: Case of Commercial Banking In Zimbabwe. *The International Journal Of Engineering And Science*, *2*(4), 34–40. Retrieved from http://www.theijes.com/papers/v2-i4/part. (2)/G0242034040.pdf

Omariba, Z. B., Masese, N. B., & Wanyembi, G. (2012). Security and Privacy of Electronic Banking. *International Journal of Computer Science Issues*, *9*(4), 432–446. Retrieved from http://ijcsi.org/papers/IJCSI-9-4-3-432-446.pdf

Osunmuyiwa, O. (2013). Online Banking and the Risks Involved, *5*(2), 50–54.

Sarma, G., & Singh, P. K. (2010). Internet Banking : Risk Analysis and Applicability of Biometric Technology for Authentication. *International Journal of Pure and Applied Sciences and Technology*, *1*(2), 67–78.

Zanoon, N., & Gharaibeh, N. K. (2013). The Impact of Customer Knowledge on the Security of E-Banking. *International Journal of Computer Science and Security (IJCSS)*, *7*(2), 81–92. Retrieved from http://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-862