Available online at www.elixirpublishers.com (Elixir International Journal)

International Business Management

Elixir Inter. Busi. Mgmt. 47 (2012) 8861-8865

ISSN: 2229-712X

Effective operational risk factors on electronic banking in Iran

Hassan Mohammadzadeubg9h Moghadam, Mostafa Akhavansaffar, Zohreh Bakhshaei and Seyed Valiollah MirHosseini
Department of Social & Economic, Payame Noor University, Tehran, I.R. of Iran.

ARTICLE INFO

Article history:
Received: 6 April 2012;
Received in revised form:
18 May 2012;
Accepted: 9 June 2012;

Keywords
Operational risk,
Electronic banking,
Security and risk reduction.

ABSTRACT

The growing trend tendency of web-based business world, emphasized on existence of an important and complementary component such as electronic banking as an undeniable necessity .In recent decades with development of communication and information tools, the volume of e-commerce significantly increased Such that between 2002 and 2006 on average each year 50% has added to the volume of trade exchange through electronic contexts. And its amount from 2,293 billion dollars in 2002 has reached to over 12,837 billion dollars in 2006. Given the widespread impact of electronic commerce and global markets dominance, it is necessary that the tools and contexts of transfer and exchange of money to keep pace with appropriate and desirable rate to the growth of e-commerce development. Adequacy of international Capital banks introduces the major risks associated with electronic banking as follows: strategic risk, credit risk, operational risk, liquidity risk, market risk and credit risk (reputation and history).One of the main identified risks in this field is that, All financial institutions Given the characteristics of the environment in which they operate And their activity amount are faced with operational risk that should be controlled As much as possible and determine the needed capital to manage it. Our main goal in this study is to identify operational risk factors in the electronic banking of Keshawarzi Bank. We first seek to identify risk factors that lead to this, so by control and reduction of impact of these factors the severity of this risk type is reduced and to bring about better management

Introduction

In recent decades with development of communication and information tools the volume of electronic Commerce in competition with traditional Commerce has had appropriate development. Banks in the field of Commercial development has given serious attention to the structural change in receipt and payment system and creating convenience in service procedures. They also have played an important role in E-commerce; because they provide the main conditions and context to establish and promoting e-commerce in the fund and credit document transfer in Internet and electronic systems. In fact Banking in the new style is known as complementary to modern Commerce and if banks don’t use electronic transaction system, a large portion of trades will be disrupted. On the other hand, participation in new trading systems in terms of technology has faced them many difficulties. Since banks should transform its service delivery system, with concert to e-commerce system. In some cases this means huge costs for the operating bank. However, success of banks in facing challenges will aid the stabilization of impact degree in electronic market. So electronic banking plays an important role in the development and evolution of, electronic Commerce. Indeed, without such field for electronic trading of money and credit documents, e-commerce cannot be sustained. In recent years The Electronic system with 24 hours of worldwide service has grown considerably, therefore dependence of this type of banking to technology to deliver services with required security And trans-national nature of the transaction, brought more risks for banks And new challenges to supervision and regulation field In banking . With clarifying the fundamental role if electronic banking in the world today. It seems very necessary to identify and control threats and risks associated with it, one of the most important risks are operational risks, that banks for the first time should set aside investment costs related to operational risk In order to identify areas of operational risk and quantify their related damage. In general for financial investment institutions risk management is located at top of priority list. in a way that In 2005, 42 percent of major financial institutions In the United States have invested between 500,000 to 5/2 million dollars on information technology for risk management. The risk is due to increased use of technology (including more reliance on foreign vendors).

Considering the process of arrival of foreign systems to our country this risk should have regard with special care. The legitimate system selection and utilizing computer science experts can greatly reduce this risk, on operational risk. Importance and necessity of research: If operational risk doesn’t manage well it not only will lead to financial losses but also can lead to bank bankruptcy. Operational risk is not a new phenomenon, but the importance of this risk is much highlighted with the spread of information technology in recent years. The goal of operational loss is reduction of frequency and the severity of events that will lead to operational losses. These activities include internal inspections and process repetition which could be utilized against abuse, theft, inaccurate pricing or damage of systems. Basel Committee announced that the principles of risk management of traditional banking system are also applicable to electronic banking activities. Only this principles should be adapted to this type of banking specifications And updated. This matter is the board and CEO of

Tele:
E-mail addresses: mmirhosseini1968@gmail.com

the banks responsibility in order to carry out measurements to revise and required reforms in policies and their risk management procedures to ensure that they covered electronic banking activities. (Basel, 2003, p. 15).

However, on operational risk should be said that some of events cannot be controlled with most powerful risk controllers. Therefore operational risk identification, prediction and disclosure of the risk source are most appropriate action in a way that it can create most value. Basel Committee also has provided the correct approach to determine required capital to control and management of this risk. The lack of an appropriate risk management approach and lack of its accurate determination of required capital not only lead to inflict of irreparable losses on the banks. But also at the long term will add to severity of other risks including credit risk, strategic risk, market risk and other bank risks. And at a consistent and increasing motion overall risk of the banks will increase. On the other hand, with accurate determination of required capital amount for operational risk management, Involvement of additional capital has avoided. And by utilization of more advanced and more accurate formulas, In addition to increasing the risk management efficiency we can benefit from capital surplus to banking operations development. For this task identification of the affecting factors of this risk and prioritizing them to development of, both advanced formula development of risk management and move toward developing management strategies to control and minimize their impact is very important.

Research objectives

The main goal: to identify factors affecting operational risk in electronic banking in banks.

Sub-goals:

1 Identify the technological infrastructure as a factor that influences the operational risk of electronic banking.

2- Identify internal control as affecting factors on the operational risk of electronic banking.

3- Identify security of as an affecting factor on operational risk in electronic banking

Research hypotheses

Hypotheses considered in the research include:

1-The technological infrastructure is effective on the operational risks in electronic banking.

2-The security factor is effective on operational risks in electronic banking.

3-Assessment and internal control factor is effective over operational risk in electronic banking.

Scope of Research

Subjective scope: This study is related to financial management field and sought to evaluate the effectiveness of the five given factors on operational risk in electronic banking industry.

Spatial scope: The scopes of this study are all branches and squad headquarters of Iran National Bank.

Time scope: the study period is preceding the 2010.

Statistical population

The Statistical population of this study has been selected Considering that in answering to intended questions Only some of the specialists within the bank Between directors and employees of Branches and keshawarzi Bank squads staff and employees that have the necessary expertise and experience of 4 years or more and have related education at of least undergraduate level And above in the field of management accounting, banking science, computer and economy Have been selected.

Data collecting tool

Data collecting tool in this study is a questionnaire. Due to specific risk management methods particular to each bank and different operating environments in Banks, there are no standard questionnaire for this purpose. And the questionnaire used in this study is based on Basel Committee's statement, about e-banking risk management that is defined and evaluated for validity and reliability by known scientific methods.

Statistical sample

In Keshawarzi Bank Branches and central offices in the Yazd province. Total of 315 individuals with B.A. and higher education degree that have the defined and required experience (at least 4 years), 124 persons have been taken from the population by the NCSS PASS software.

Data analysis method

In the present study, analysis of of data is based on Friedman test rate and Kruskal-Wallis test and Spearman correlation coefficient test. Cronbach alpha has been used in analysis of data in the SPSS software to determine the reliability of questionnaire.

Inferential statistics

First hypothesis

There is a relationship between operational risks reduction and technological infrastructure

HypothesisH_0: There is no relationship between operational risk reduction and technological infrastructure

HypothesisH_1: There is a relationship between operational risk reduction and technological infrastructure.

According to significance of test in one percent level the hypothesisH_0 declined and the hypothesis H_1 is accepted. Thus there is a relationship between technological infrastructures. And operational risk reduction obtained Asprmn value indicates an Inverse relationship between technological infrastructure and operational risk reduction. In other words, increase in technological infrastructure will reduce operational risk.

The results of Friedman test show that among the questions 1 to 5 for the technological infrastructure variable Question (telecommunication network development) has the highest rating

Second hypothesis

There is a relationship between reduction of internal controls and operational risk reduction

Hypothesis H_0: There is no relationship between internal controls and operational risk reduction

Hypothesis H_1: There is a relationship between internal controls and operational risk reduction.

There is a relationship between reduction of internal controls and operational risk reduction

Hypothesis H_0: There is no relationship between internal controls and operational risk reduction.

Hypothesis H_1: There is a relationship between internal controls and operational risk reduction.

According to significance of test in one percent level the hypothesisH_0 declined and the hypothesis H_1 is accepted. Thus there is a relationship between internal controls. And operational risk reduction obtained Aspreman value indicates an Inverse relationship between internal controls. And operational risk reduction. In other words, increase in internal control. Will reduce operational risk.

The results show that in the Friedman test questions from 1 to 5 for internal controls variable Question (control over permit of customer's entrance to electronic banking system and customer authentication) has the highest rating.

Thirds hypothesis:

There is a relationship between reduction of domain security and operational risk reduction.

Hypothesis H_0: There is no relationship between domain security and operational risk reduction.

Hypothesis H_1: There is a relationship between domain security and operational risk reduction.

According to significance of test in one percent level the hypothesis H_0declined and the hypothesis H_1 is accepted. Thus there is a relationship between domain securities. And operational risk reduction obtained Aspreman value indicates an Inverse relationship between domain security and operational risk reduction. In other words, increase in domain security will reduce operational risk.

The results show that in the Friedman test questions from 1 to 6 for domain security variable Question (software protection to prevent unauthorized intrusion to the systems) has the highest rating

According to above tables , Krskal Wallis test has been significant at one percent level. Thus, risk there is a difference between internal controls, technology infrastructure, and security domain variables to reduce operational risk, from Table 4 -16 can be seen security has earned the highest rating. Therefore increasing the security has the most effect on reducing operational risk.

Conclusion:

According to hypothesis testing based on assumptions 1 to 3 of Research results, the three factors "security, internal control and technological infrastructure. "Are affecting the operational risk of Keshawarzi Bank's electronic banking and According to each factor of test components identify all three under study as effective factors on operational risk of electronic banking in Keshawarzi Bank.

Research hypotheses Test results

by comparing The research hypotheses Test results we conclude That importance of "security" factor in Reducing operational risk at the Keshawarzi Bank Electronic banking is more than other factors. And "internal controls" factor is if higher degree of important compared to technological infrastructure factor.

The studied Component variables Assessment

1) By study the component Assessment in technological infrastructure. And ranking Them it is concluded that All components has effect over operational risk of electronic banking systems in Keshawarzi Bank .And except for "SWIFT network development "and "equipment ATM development " " components that are of Secondary priority, "networks performance", " level of technology used in credit cards. "And "development of telecommunications networks" Components has equal priority and is of first degree of importance.

2) By Assessment of studied components in "internal control" areas and ranking them it is concluded that all components are effective over operational risk in electronic banking systems. Of Agricultural Bank Thus "internal controls" areas factors are in two degrees of importance. First degree consists of the following three factors:

- Control over customers Entering permit issuance to electronic banking system and customer authentication.
- Physical control of servers and database systems

-controlling the opening, changing and closing of a customer account

3)by components Assessment in field of "security" and rating Them its concluded that All components has effect over operational risk of electronic banking in Keshawarzi bank.

And among the six under study components of field security on impact, According to their average rank can be divided into three grades of .importance.

"Protecting software for unauthorized intrusion into the systems" And " management of software development and security systems" are of First degree of the importance And secondary importance includes "performing periodic security Assessment of people in key posts," "existence of anti-virus software and network periodic penetration tests." And third degree of importance includes "sensitive data classify ".

References:

[1] Azar, Adel. Momeni,mansor., (1380) Statistics and Its Application in Management, Volume II, Fifth printing. Tehran: Samt publication

[2] Bazargan, Abbas, Sarmad, zohreh, Hejazi, elahe (1379), Research methods in behavioural sciences, third printing, Tehran, Agah publication

[3] Monetary and Banking Research, (1384) Electronic banking services and administrative measures, First printing, Tehran.

[4] Hassanzadeh, Ali, (1382). Risk management in electronic transactions, Journal of New Economics, Volume 100, page15-18.

[5] Razeghi oskoui, Faranak (1382) Electronic banking services in the country, Informatics Newsletter, Volume 94, page12-13.

[6] Oghlori, Ahmad, Erfanian, Amir (1385), Comparative study and implementation of operational risk measurement models adopted in the Basel Committee on Sanatomadan Bank, Sharif Journal, Volume 9422mpage 1-17.

[7] Abbasinejad, Hossein, Mehrnoosh, mina (1385), Electronic banking book, Tehran, Samt publication.

[8] Basel committee. (2003). Risk Management for Electronic Banking Basel. Switzerland: Bank for International Settlements.

[9] Basel committee. (2003). Supervisory Guidance on Operational Risk Advanced Measurement Approaches for Regulatory Capital.

[10] Rostinah Supinaha, Zuraidah Anisb, Hanudin Amina (2008) Banking Channels Adoption in Malaysia: an analysis.

[11] Cornalba, Chiara. Giudici, Paolo. (2004). "Statically Model for Operational Risk Management". Physical A.No 338, PP 166-172.

Appendix

Table 1 - Description of education level

Education	Frequency	Frequency Percent	Cumulative frequency percent
Bs	96	42/77	42/77
Ms	28	58/22	100
Total	124	100	

Table 2 - description of field of study

Field	Frequency	Frequency Percent	Cumulative frequency percent
economy	14	29/11	29/11
Accounting	30	16/24	48/35
Banking Sciences	18	52/14	50
Computer	16	9/12	9/62
management	46	1/37	100
Total	124	100	

Table 3 - description of work experience

Experience (year)	Frequency	Frequency Percent	Cumulative frequency percent
4-7	36	03/29	03/29
8-14	63	81/50	83/79
15-23	25	16/20	100
Total	124	100	

Table 4 - description of technological infrastructure variable

description	Frequency	Frequency Percent	Cumulative frequency percent
Very low	0	0	0
low	20	22/3	22/3
Somewhat	122	68/19	9/22
high	228	77/36	67/59
Very high	250	32/40	100
Total	620	100	

Table 5 - description of internal control variable

description	Frequency	Frequency Percent	Cumulative frequency percent
Very low	0	0	0
low	21	38/3	38/3
Somewhat	71	45/11	83/14
high	260	94/41	77/56
Very high	268	23/43	100
Total	620	100	

Table 6 - description of security variable

description	Frequency	Frequency Percent	Cumulative frequency percent
Very low	0	0	0
low	29	89/3	89/3
Somewhat	83	16/11	053/15
high	251	74/33	79/48
Very high	381	21/51	100
Total	744	100	

Table 7 - Spearman test for the first hypothesis

Significant level	number	Spearman value
001/0	124	527/0-

Table 8 - Friedman test for comparison of a within group of technological infrastructure

Significant level	test value	Degrees of freedom	Type and number of test
000/0	18/95	4	Friedman
		124	total

Table 10 - Spearman test for the second hypothesis

Significant level	number	Spearman value
000/0	124	623/0-

Table 11 - comparison of Friedman test for internal controls within a group

Significant level	test value	Degrees of freedom	Type and number of test
000/0	46/110	4	Friedman
		124	total

Table 12 - Questions 1 to 5 for a description of the Friedman test

question	rank
Electronic banking transactions tracking	68/2
Account activity by customer : Account Control, open new account ,close an account ...	06/3
Log on licensing control system for electronic banking customers to customer credit confirmation	46/3
control Personnel access to system	64/2
physical controls of data base servers and systems	16/3

Table 13- Spearman test for the thirds hypothesis

Significant level	number	Spearman value
000/0	124	711/0-

Table 14 - Friedman test for comparison of within-group domain security

Significant level	test value	Degrees of freedom	Type and number of test
000/0	84/142	5	Friedman
		124	total

Table 15 - a description Questions 1 to 6 for of the Friedman test

question	rank
Periodic safety of people in key posts	38/3
There is software protection to prevent unauthorized intrusion into computer systems	10/4
Periodic network penetration tests	11/3
There is an anti-virus software	43/3
Classification of sensitive data	02/3
Management update of software and systems security	96/3

Table 16 - a description of Krskal Wallis test for comparing the Research's three independent variables

Average ranks	Number of sample	variable
09/334	124	Internal controls
52/312	124	Technology infrastructure
29/348	124	Security scope

Table 17 - Krskal Wallis test for comparison of independent Research Variables

Significant level	Degrees of freedom	chi^2 value
001/0	4	99/19