

Risk Management Strategies of Electronic Services in the Iran's Banking System

Rosa Khezri and Ruhollah Tavallaei

Abstract—The current study is undertaken with the objective to examine risk and the strategies of its management for electronic banking services in Iran. Continuous innovation in the field of communication and information and also competition between banks has resulted to the fact that banks increasingly provide wider electronic facilities to their macro and micro customers and this vast expansion of capabilities and abilities of electronic banking has various advantages and perils. Hence, it is necessary that these hazards in the banking systems are identified and strategies for management of risk in electronic banking be provided.

Therefore, in this study, after examination of theoretical literature review and also examination of documents of the new electronic banking in Iran, the existing risks in the electronic banking are recognized and categorized. Then with the help of the Delphi method and also taking views of 14 experts in the field of information technology in Iran's banking system, 45 strategies of risk management of electronic service are identified in or order to be implemented in the Iranian banking systems and are categorized into two group; short term strategies (28 strategies with first priority) and mid-term strategies (17 strategies with second priority).

Index Terms—Banking system, Delphi method, electronic banking, electronic service, risk management.

I. INTRODUCTION

Electronic banking consists of providing means for employees in order to increase their speed and efficiency in providing banking services and also process of inter-branches and inter-banks across the world, and providing software and hardware services for the customers so that they can do their banking operations through safe and secure channels, 24 hours a day, without being needed to be physically present in the bank. Electronic banking consists of usage of advanced software and hardware technologies that are based on the net and communication, in order to exchange resources and financial information's electronically and also does not require the physical presence of the customer in the branch.

One of the required and necessary instruments for making electronic commerce possible and also its expansion is the existence of electronic banking, which along the global financial and monetary systems, makes possible the activities related to electronic commerce. With wide usage of computers, information technology, net technology and computerization of data, electronic commerce provides this

chance for the companies so that they can enhance their financial process in sales, purchase and also internal activities [1].

Continuation of innovations in technology and competition between the existing bank organizations and new entries, has provided this opportunity so that wider line of services and bank products be available and through distribution electronic channels to their macro and micro customers and under the title of electronic banking be given to customers. New technologies and electrocution of banking, gives this possibility to banks and financial institutions to enhance and increase their speed, quality, precision, cost and diversity [2].

However, speedy development of electronic banking capabilities, in addition to its advantages has various perils and risks. In order to minimize the perils and legal and credit risks of the electronic banking, banks must undertake to disclose information on their websites and also provide suitable Scale for indicating their loyalty to the private sphere of the customers in the legal and juridical field [3].

II. THE NECESSITY AND IMPORTANCE OF THE STUDY

One of the most important global associations in the field of banking is the "Basel Committee". This committee is consisted of the high representatives of the countries of G10 and usually once every three months the Bank for International Settlements is considered as secretariat and the meetings are convened in the city of Basel, in Switzerland. This committee does not have legal power, but most of the member countries are implicitly bound to perform and undertake its suggestions [4].

The Basel overseeing committee expects that the existing perils in electronic banking systems are identified and with prudent manner and also based on the nature and characteristics of electronic banking are managed by the banks [5]. These characteristics consist of the unprecedented speed of change in the field of technology and innovations related to services provided to the customers, the specific and global nature of open global electronic net, and unification electronic banking programs with computer systems and increase of the dependence of the banks to the companies that provide information technology. Although the risks related to electronic banking are not created quintessentially, but the Basel committee believes that the characteristics of electronic banking causes increase and change in some of the usual risks in banking activities such as operational risks, legal and known risks and in sum the total risks of the banks.

Considering the mentioned discussions, in addition to undertaking of the current foundations of the existing risks in electronic banking, it is necessary that these foundations are

Manuscript received September 10, 2014; revised October 30, 2014.

Rosa Khezri is with the Islamic Azad University, Iran (e-mail: rosa_khezri@yahoo.com).

Ruhollah Tavallaei is with the Shahid Beheshti University, I.R.Iran (e-mail: r_tavallaei@sbu.ac.ir).

made compatible with the characteristics of electronic banking and are expanded based on and in accordance with the challenges of the management of risks. Based on this, the Basel committee believes that the managing committees and the higher committees of banks must undertake steps in order to ensure change and revision in the foundations of current risk management based on electronic banking and also the processes in order to cover these activities at present and in future. Moreover, integration of the applied electronic banking programs with current banking systems consists of an integrated risk management strategies for all of the activities of a bank. The credit results of lack of consideration to examination and control of risks in banks, specifically electronic banking is very costly and hence it is necessary that all banks of the country be ready with the necessary steps and remedies in order to be able to cope and face the possible risks in electronic banking systems [6].

III. METHODOLOGY OF THE STUDY

This study, according to its objective is an applied one, and it is so because, it is focused on the line of acquiring information on the existing risks in electronic banking service and these information are useful for the concerned organization and decision making in this field.

Moreover, in order to gather information in this research the following methods are used: Library and document reading studies, and 2- Delphi technique. One of the ways of acquiring collective knowledge is usage of Delphi technique that is a process which has a structure in order to forecast and helps decision making in Survey rounds, information gathering and also finally collective consensus [7]. Hence, the researcher in this study, based on the stages of a Delphi study have undertaken the following steps:

- 1) With the help of library and document reading books, the existing risks in the electronic banking system of Iran were identified.
- 2) Usage of Delphi techniques in order to make a correct interaction between real expert ideas that were studied. Hence, for this reason, the identified risks were given to 14 experts based on choice and judgment and it was asked from them to provide their ideas about the strategies of risk management.
- 3) Examination of ideas. Because the Delphi technique seeks consensus between experts, after gathering of the answers, the ideas of the respondents were analyzed and examined. In this study the Priority index and Consensus Index were used, so after analyzing the returned questionnaire in the first round, the questionnaires of the second round would be done, according to the discrepancies in the ideas of the experts. Afterwards, according to the results of analyzing the questionnaire and taking conclusion, the findings of research are given.

IV. THE FINDINGS OF RESEARCH

The findings of the current research are given under two categories. A) Identification of existing risks in existing

electronic banking service B) strategies of existing risk management in electronic banking system:

A. Identification of Current and Existing Risks in Electronic Banking

Based on the findings of the current research, the current risks in electronic banking service can indicated and categorized in the following chart Fig. 1:

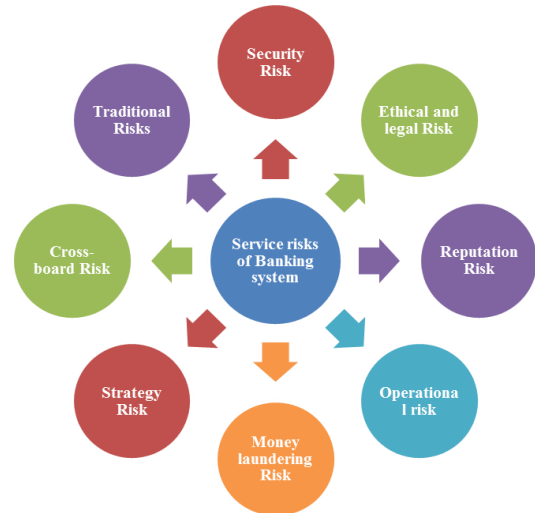


Fig. 1. Categorization of existing risks in electronic banking system.

As it is indicated in the above diagram, these risks are categorized into eight groups:

- 1) Security risks: this risk is due to the danger of hackers, virus and collusion between the employees and in order to reduce this risk, persistent overseeing, specifically in crisis times, over banking operations is required.
- 2) Legal and ethical risk: this risk is indicative of weakness in law making and existence of vague laws. Moreover, it considers the cases of escaping from the law. The importance of this risk is seen more in relation to the weakness of laws regarding overseeing and control.
- 3) Reputational risk: this risk is related to the reputation of banks in providing electronic service. Damage to the reputation of bank has negative effects in society and results in damage in the relationship between bank and customer and reduction in the number of customers. This risk is resulted either from weak performance of bank in providing electronic service or weakness in providing communicational services of the country and the result of both is lack of satisfaction of customer and lack of thrust in them.
- 4) Operational risk: this risk is resulted from weakness in designing the system, weakness in control and overseeing the banking information system and also weakness in employing human resources. Part of this risk is related to electronic banking system and the other part is related to employment system of the bank.
- 5) Money laundering risk: this risk is related to the weakness in identifying the customers and also weakness in internal accountability. Recognition and identification of customers, specifically key customers and strengthening of examination, overseeing and electronic data control structures, by the internal overseers, in this case is necessary.

- 6) Strategy risk: it is related to productions and new services in electronic banking system. Wrong estimation of expansion costs or creation of new operations, lack of adequate branch employees in order to support the operation and lack of coverage are important factors in this risk.
- 7) Cross-board risk: This risk indicates various risks and also combined risks that include market and economic risk that can increase the risk of expansion of electronic banking system. In other words, this risk is concerned with the uncertain economic and financial risk. Weakness in laws concerning protection of customer in the country, vague law making and financial operations, lack of providing report information, differences in economic, cultural, social, political conditions of other countries in exchange rates and electronic banking operations between banks, branches and international

- banks are the reasons for this risk and also the risk of exchange rate are important factors in this case. This is an external risk that is imposed upon the electronic systems of the banks [8].
- 8) Traditional risks: this indicates traditional risks such as liquidity, market risk, rate of interest risk and credit risk that can be influential on the electronic banking system [9].

B. Strategies of Management of Risks Electronic Services of the Banking System

Based on the findings of the current study, the suggested Strategies in order to manage the existing and current risks in electronic banking system can be categorized as following Table I:

TABLE I: STRATEGIES OF RISK MANAGEMENT IN ELECTRONIC BANKING SYSTEM

Risk title	Strategies of Risk management	
	Short term priority	Mid term priority
1 Security Risk	1. determination of security standards for the used software and hardware 2. Execution of detecting systems with SOC and CSIRT capabilities 3. Digital signature 4. Usage of Socket Secure Layer 5. Integration and unification pay bases 6. Proxy double checking 7. Record of all changes 8. Usage of different coding for transfer of information	9. Execution of ISMS 10. Designing and execution of local performances such as NIST 11. Execution of rules of PCI and DSS
2 Ethical and legal risk	12. Clarification of laws 13. Making execution guarantee for performance of laws 14. Revision of rules and laws of Banking system 15. Informing the customers and employees	16. Formation of RRD 17. Solving the ambiguities of laws and rules and integrating them
3 Reputation Risk	18. Creation of the box of compensation for financial investors 19. Enhancement of SLA in the inter banking transmission net of information	20. Updating and continuous expansion the specific Bandwidth of the banks in accordance with their needs.
4 Operational risks	21. fine for losses resulted from wrong file making 22. Enhancement of SLA 23. creation of strategies for reduction of the effects of risks 24. Employment of individuals who have necessary skills in electronic banking	25. Educational training 26. System overseeing(entry of data, data processing, exit of information) over banking system
5 Money laundering risk	27. Creation of laws and rules visa-vis money laundering in the form of complete booklet 28. inquiring data and designing an intelligent system of money laundering	29. Usage of AML instruments 30. Creation of Fraud detection in bank's systems
6 Strategy risks	31. creation of a group for examining the new electronic service. 32. Taking into consideration, the legal issues that are bidding in expansion of new electronic system	33. creation of a group for future research. 34. personalization of banking products.
7 Cross board risks	35. Dealing with changes in the foreign exchange rates 36. Designing intelligent B.I electronic system in order to analyze the processes governing the economy 37. Control of the open situation	38. Usage of PESTA analysis in expansion of new electronic services 39. Common information exchange between different sectors of bank, insurance and stock
8 Traditional risks	40. creation of internal accountability committees. 41. considering the governing laws of company. 42. Usage of stress testing systems and speedy warning systems	43. creation of credit rating of legal and real customers companies 44. Determination of adequacy of funding in macro activities of banks based on the suggestions of the new Basel committee 45. Considering the micro resources and consumptions of banks

As it is shown in the above diagram, based on the findings of the current study, the most important strategies of risk management in electronic banking services, that have obtained the highest scores in this study in the findings of the Delphi method are as following:

Strategies of security risk management. The short term

strategies of this risk are as following:

- 1) Determination of security standards for used software and hardware:

Business, commerce and electronic banking require various contexts such as the use of software. Independence of the web related programs to the platform and executive

capacity of them in the internet at all points results in reduction unnecessary costs that results from virtualization of the systems. Boom of the service provider and service taker programs and also expansion of the powerful data base in the service providers, with the integration capacity and use of the advanced coding methods and also usage of safe and secure protocols and firewalls (for security of information and providing and back up capabilities from information), results in safety and security of the customer and banks.

2) Execution of detecting systems with SOC and CSIRT capabilities:

This is a emergency center for responding to the instances of information security that might happen in the banking network. This is based on the achievements and CSIRT and SOC capabilities. Establishment CSIRT in organizations as a security base- structure includes skilful human resources, security technology and related processes and it empowers the organization against cyber-attacks and decreases their vulnerability visa-vis such attacks. Security operation center is monitoring and control of security.

3) Digital signatures:

It is a form of incongruent coding. This is used in order to generate a digital signature from a mathematical algorithm in order to combine information in a click with the message information.

4) Usage of Socket Secure Layer:

This is a standard web for coding the information between the user and the website. Information that are exchanged through the SSL connection, are exchanged as codes and hence they are protected from being stealed or eavesdropped.

5) Integration and unification pay passes:

It is a system that manages the withdraw and deposit, and sends the results to the machine card readers. In order to deal with the payment of the website's fishing it uses a disposable password (OTP). This is similar to the Shaparak system.

6) Proxy double checking:

It records the traffic proxy of the internet and intra-net. For example a talent server proxy, traces every strike on the keyboard in every talent in the internet and also it can examine the circumstances of encountering an external server against the click pressings. The proxy can also examine and record each and every IP address, its date and time of accessibility an URL and even the transmitted bites. These information can be used against any possible threat and attacks that is done against the network. The firewalls create a single layer or a protective shell around the computer or create these around the network visa-vis the destructive codes and unnecessary traffic. However, it does not guarantee your system against the attacks. Usage of firewalls along with other kinds of protective measures such as anti-virus software and taking into consideration the security measures can have positive effects regarding the protective level of your computer and also your system.

7) Record of all changes:

This is for recording of all transactions done in the electronic banking system in order to overcome and also predict the system's risks.

8) Usage of different coding for transfer of information:

In order to prevent abusing of the banking system and also

keep the security of transmitted information in the network, new coding methods are used.

Also, the long term strategies of risks are as following:

9) Execution of ISMS:

The managing of security of information is stated with the following objectives: indicating and explaining clear safety measures in order to manage the information security risks of the companies in the framework of work's risks and under the title of assessment , Guidance and support of intra and inter organizational information security at an agreed level. The stages of designing and execution of the system is not necessarily sequential and could have overlapping. Creation of a context in order to create coordination between all personnel's of the project in order to take steps in direction of providing information security of the organization.

10) Designing and execution of local performances such as NIST:

For this point the following points should be taken into consideration:

Identification, protection and disclosure and also responses to and circumstances of the restoration resulted from a cyber-attack. This central part requires a high level of managerial point of view for the industries.

This framework has a part that attempts to model the present situation of an organization, from the cyber security point of view. This is in order to let the security team know which parts have alarming situation and its aim is to match these parts with the current advanced set of threats.

This cyber system attempts to take into consideration the needs of the businesses. With regard to the explanation of the framework it says that the introduced system is a adaptive of standards, rules and methods of execution of this framework.

11) Execution of rules of PCI and DSS:

It is a set of comprehensive rules for advancement of the security of the system that are made for the industry of the payment cards. PCI DSS is a standard of information security, in which every business should to some extent receive it for the usage of payment cards and also savings, processing or sending of information of the card holder [10].

Strategies of Ethical and legal risks management. The short terms management of this risk are as following:

1) Clarification of laws:

These are related to the disclosure of realities and systematic discipline of the rules regarding transparency.

2) Making execution guarantee for performance of law:

Guarantee in performance of the laws is the most significant rule regarding obligation in performance. Limitations and sanctions, exclusions and heavy fines are examples of this case.

3) Revision of rules and laws of banking system:

Congruent laws and execution capacity, justifiability, and economical rules are effective in reduction of lawful and ethical risks.

4) Informing the customers and employees:

Increasing the level personnel and customers understanding regarding usage of electronic banking services.

Moreover, the short term management of these risks are as following:

5) Formation of RRD:

Regulation Reference Database (RRD): It is a data base that all rules are recorded in it, in order to record all rules min it so to control the laws and rules in a systematic way.

6) Solving the ambiguities of laws and rules and integrating them:

There are various ambiguities in the rules that can be abused by various individuals.

Strategies of reputation risks management. The short term strategies of the management of this risk are as following:

1) Creation of the box of comprehension for financial investors:

There is this possibility for the customers that in case of lack of ability of the bank in order to fulfill its financial obligation, they can receive the losses.

2) Enhancement of the SLA in the inter banking transmission net of information:

It is a service level agreement, which is an agreement for guaranteeing and providing a specific level of quality of services, from the side of the service provider company for the company that receives the service or the user.

The long terms management strategies of this risk are as following:

3) Updating and continuous expansion of the specific Bandwidth of the banks in accordance with their needs.

Strategies of operational risk management. The short terms management of this risk are as following:

1) Fine for losses resulted from wrong file making:

If a bank enters a wrong file or even records in the inter banking system, it will be subject to monetary fine.

2) Enhancement of SLA:

It is a service level agreement, which is an agreement of guaranteeing and providing a specific level of quality services from the side of the service provider company for the service receiver company or the user.

3) Creation of strategies for reduction of the effects of risks:

Examination of the interim risks, frauds, human errors, penetration and control and reduction of all operation systematic and non- systematic risks, results in increase in the fame, self -reliance and reliability and credibility of the bank.

4) Employment of individuals who have necessary skills in electronic banking:

The bank's personnel must have necessary and required skills with regard to computer usage and also should be familiar with the latest advancements in the information technologies in the context of banking system.

In addition, the long term strategies of risk managements are as following:

5) Educational training:

Trainings regarding the internet banking system; systems of code writing of internet banking, training courses for specialized systems and new technologies of banking industry.

6) System overseeing over banking system:

Usage of overseers and having overseeing systems (entry of data, processing of data, exit of information) and also usage of the fast alarming systems and also under pressure tests.

Strategies of money laundering risks management. The short terms strategies of this risk are as following:

1) Creation of laws and rules visa-vis money laundering in the form of complete booklet:

Management of risks related to money laundering in banking operations is possible with the use of the suggested remedial methods given by the I.M.F and the ball committee.

2) Inquiring data and designing an intelligent system of money laundering:

Inquiring the data and creation of intelligent systems is very effective in order to classify the customers and predicting the behaviors of the customers.

Moreover, the long term strategies of the management of this risk are as following:

3) Usage of AML instruments:

Anti- Money laundering (AML): It was formed with the objective of coordination of the organizations related to collection, processing and analysis of the news, documents, information and the received reports, providing intelligent system, suspected transactions with the objective of overcoming the crime of money-laundering.

4) Creation of Fraud detection in bank's systems:

This is to speed up the operation regarding the identification of fraud related activity. Generally, the methods of identification frauds are divided into two main dissonances and abused identification:

In abnormal identification the history of the customer's behavior is considered as normal and any kind of deviance from this normal behavior is considered as dissonant and abnormal behavior or can be recorded as fraud. The method of identification of the abuse is focused on the specific behaviors of the customer and assumes known behaviors as fraud.

Fraud in electronic banking occurs in the context of electronic services and occurs online and the result of this is the illegal electronic transaction of money from an account to another account that imposes various kinds of losses to the banks.

The management of risk strategies. The short term strategies of this risk management are as following:

1) Creation of a group for examining the new electronic services:

Pre-study of creation of strategies and logical cost benefit analysis and the required technical and economic justification are necessary factors for creation of strategies regarding electronic banking.

2) Taking into consideration, the legal issues that are bidding in expansion of new electronic system:

Perhaps the emergence of electronic banking is the most effective and influential factor in changing and re-shaping of the banking sector. Hence, laws and regulations should change regarding the capacities of the electronic banking and be created along these changes.

3) Creation of a group for future research:

The banking system, along with the changes in the market and also the global advancements has changed rapidly into the electronic banking system (the expansion of new banking products based on the latest technologies of the world) and hence in this regard has obtained various advancements. On these lines, identification of the customers need and requirements and providing related electronic banking

systems that is based on current needs and also forecasting of such needs and risks in future is very significant. The financial markets are not stationary and solid. The new technology provides a platform to discover the dynamics of the markets and also creation related products based on these dynamics.

4) Personalization of banking products:

Creation of creativity in various products and banking services and also making differentiation in providing these services, is along with increase in speed, quality and precision of the customer.

Strategies of Cross board risks management. The short term strategies of this risk are as following:

1) Dealing with changes in the foreign exchange rates:

Keeping the value of the national currency assist to provide healthy financial requirements of production activities and also overcoming the needs of the society. This is possible with the creation of a stable macro- economic atmosphere, reduction of inflation and also overcoming the inflationary expectations that ultimately results in stability in economic activities.

2) Designing intelligent B.I electronic system in order to analyze the processes governing the economy:

This is used to analyze the overall governing condition of the economy.

3) Control of the open situation:

Identification of transactions that due to any reason have not been done correctly in the banking system and also finding ways and mechanisms to resolve these issues.

4) Usage of PEST analysis in expansion of new electronic services:

Identification of the environment that the bank operates in it, in order to identify and outline the strategies and executing them, political issues, economic issues, social issues and technological issues.

5) Common information exchange between different sectors of bank, insurance and stock:

Connecting with organizations and companies that have close relationship with the banking network, in order to have direct, uncontrolled relationship, so to avoid any kind of abuse.

Strategies of traditional risks management. Short term management of these risks are as following:

1) Creation of internal accountability committees:

Many of the violations and breaches that are done through giving forgery documents will be overcome by this measure.

2) Considering the governing laws of the company:

Creation of standards and controlled limitations for directing and control of the intermediary financial institutions, such that can protect the interests of all beneficiaries. This will reduce the costs and risks and hence results in protection of their interests. This measure results in the fact that bank will have a better operation and reaction in crisis time, in order to make transition to stable situation. Hence, assists them to a large extend to be safe from bankruptcy. Considering the economic and legal challenges that results in crisis in the banking system and hence in breaking of the situation and speeding up of the bad economic situation, it will causes these problems to move in between societies. Therefore, it is necessary to recognize the

main factors that create such situations for these institutions, and by controlling them through viable and correct political measures and policies, a possibility of protecting the rights of the concerned individuals would be made possible (depositors, stock holders and the party sides) and hence it results in economic stability in the society and economy.

3) Usage of stress testing systems and speedy warning systems:

This is used and is possible for the identification of problems within the structure and architecture of the applied program, recognition of the effect of a software or hardware over the overall effectiveness of general programs used in the banks, specifically when the load of the system is at the maximum level and also in the long run. It is also possible for recognition of unusual and suspicious actions of users with the intelligent system.

The long term strategies of the management of this risk are as following:

4) Creation of credit rating of legal and real customers companies:

For rating and examining the credit risks, companies are usually organized based on the risks that are mentioned in the agreement. This is referred to as rating. In order to measure the credit rating, every rate is given a Nokoli probability. A credit rating company (Credit Bureau) through providing credit rating system and rating, is responsible for advancement of the credit system of a country. Using the services of the company results in the fact that credit provider companies can know about the past and present situation of their customers in the entire banking system and hence they can make their credit decisions in the least possible time and in the speediest fashion.

5) Determination of adequacy of funding in macro activities of banks based on the suggestions of the new Basel committee:

The drafting committee in the international liquidation bank (BIS) has named it international congruency in measuring capital and the governing standards. It has also examined the best ratio of adequacy of capital in the bank, by analyzing the comparative level of adequacy of capital in some of the axioms of the regional banks and hence has offered various preventive measures for the financial crisis.

6) Considering the micro resources and consumptions of banks:

Many of the violation and breaching that is done through forgery of documents can be overcome by this method. The operational and control system can trace the current transactions based on the existing laws and rules and hence all transactions in the banking network can be under scrutiny. In reality with the assistance of the scrutinization capacity of the electronic banking system and also based on the transaction data of the banks, we are able to recognize quickly their situation.

V. CONCLUSION

The electronic banking due to its vastness and its slogan of "everybody" and "everywhere" has specific characteristics and hence does have various risks and perils. Some of the important indicators in increase of risk are as following:

technological changes, changes in the expectations of customers, increase in the level of net access to the public, decrease in face to face interaction between customers and institutions, necessity of integration of electronic banking systems with computer systems of institutions. In order not to face these dangers, some institutions might not provide some of these services or otherwise, provide limited services via informing websites. The latter approach, of course in today's world that is marked by new technologies, can cause the company to lag behind the competitors and loss of their customers.

On the same line, it was tried in this study to first identify the risks involved in electronic banking and hence categorizing these under 8 different groups. Then, with the usage of Delphi method and also the survey from experts of this area, suggested mechanisms and strategies for short term (28 strategies with first priority) and mid-term strategies (17 strategies with second priority) are provided to be executed in the banking systems.

Usage of international standards such as FMI and Bassel I/II/III and also considering the suggestions of the BIS can be helpful in reduction of the mentioned risks. Another point to be considered in this regard is creation of identification and examination of risk committees in the banks. This is so because in today's banking, the concepts of bank and banker are not similar to the past that was limited to intermediaries of funds. In reality, the banker, in today's world is the manager of the risks.

REFERENCES

- [1] EBC. (2005). E-business connection. *Critical Success Factors for e-Business*. [Online]. pp. 1-5. Available: <http://www.e-bc.ca>
- [2] E. Turban, D. King, and D. Viehland, *Electronic Commerce: A Managerial Perspective*, 1st ed., Upper Saddle River: Prentice-Hall, 2006, ch. 1, pp. 1-24.

- [3] A. Tanveer, "Electronic customer relationship management in online banking," Report of Department of Business Administration and Social Sciences in BIS, pp. 19-54, 2009.
- [4] C. H. Marrison, *The Fundamentals of Risk Measurement*, 1st ed., New York: McGraw Hill, 2002, ch. 5, pp. 340-342.
- [5] M. Roshandel, "Risk management principles for electronic banking," Central Bank of the Islamic Republic of Iran, 2009.
- [6] O. Lustsik, "Can e-banking services be profitable?" Working Paper, Tartu University Press, 2004.
- [7] L. Ludwig and S. Starr, "Library as place: Results of a Delphi study," *Journal of the Medical Library Association*, vol. 93, no. 3, pp. 315-316, 2005.
- [8] F. Vargas. (October 2013). Principles for effective risk data aggregation and risk reporting. *Bank for International Settlements*. [Online]. Available: <http://www.bis.org>
- [9] S. Zarei, "Risk management of internet banking," presented at the Recent Researches in Artificial Intelligence. 10th WSEAS International conference on Artificial Intelligence, Knowledge Engineering and Data Bases (AIKED 11), Cambridge, UK, February 15-16, 2011.
- [10] G. Johnson. (October 2002). Management and supervision of cross-border electronic banking activities. *Bank for International Settlements*. [Online]. Available: <http://www.bis.org>



Rosa Khezri is a student of eMBA, Islamic Azad University and was born in 1976 in Tehran city. She is from System Analyst Central Bank of Iran (CBI), since February 2000 up to now, I.R.Iran. Her research interests are in fields of knowledge management and ICT.



Ruhollah Tavallaee is a researcher and supervisor in this research. He was born in 1984 in Shiraz city, I.R.Iran. He is a PhD graduate of production and operations management and a faculty member of Shahid Beheshti University (Information Technology Management Group). His research interests are in fields of knowledge management and ICT.