American Journal of Computer Science and Technology
2018; 1(1): 31-38
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20180101.15

Developing a Conceptual Model for Applying the Principles of Crisis Management for Risk Reduction on Electronic Banking

Maedeh Babaei Chafjiri[1], Abbas Mahmoudabadi[2]

[1]Department of Information Technology and E-commerce, MehrAstan University, Guilan, Iran
[2]Department of Industrial Engineering, MehrAstan University, Guilan, Iran

Email address:
babaei@mehrastan.ac.ir (M. B. Chafjiri), mahmoudabadi@mehrastan.ac.ir (A. Mahmoudabadi)

To cite this article:
Maedeh Babaei Chafjiri, Abbas Mahmoudabadi. Developing a Conceptual Model for Applying the Principles of Crisis Management for Risk Reduction on Electronic Banking. *American Journal of Computer Science and Technology*. Vol. 1, No. 1, 2018, pp. 31-38.
doi: 10.11648/j.ajcst.20180101.15

Received: October 30, 2017; **Accepted**: November 20, 2017; **Published**: January 2, 2018

Abstract: Despite many benefits of e-banking for customers, operators and bank managers, e-banking activities are associated with some kinds (types) of risks. Therefore, it is essential to manage E-banking risks utilizing the concepts of risk reduction techniques such as crisis management. The main aim of the present research work is to utilize the principles of crisis management for risk reduction in e-banking. Major risks associated to e-banking including security, provisional, operational, reputational, legal and strategic activities have been identified at the first stage followed by developing a conceptual model for the application of crisis management countermeasures to reduce the risks of electronic banking activities at the second stage. The proposed conceptual model has been validated by analyzing the filled out questionnaires designed for this purpose. In addition to conceptual model approval, results revealed that the principles of crisis management could be applied to reduce the risks which are associated with e-banking activities for both customer relations and internal transactions.

Keywords: Electronic Banking, Electronic Banking (E-Banking) Risks, Crisis Management, Conceptual Modeling

1. Introduction

The existence of an efficient banking system is essential for entering and active presence in global markets and enjoying a great deal of e-commerce activities. E-commerce can provide financial interactions for both domestic and foreign customers along with other advanced banks over the world. Moving from manual to fully computerized processing and increasing processing capacity has increased risk involvement, which is the most worrying concern of banking activists. This is getting to be more important when the use of electronic systems in financial and credit institutions has being rapidly expanded [1] and the number of users of electronic banking services is increasing day to day as well. Increasing the number of users can be known as a double-sided consideration of opportunity and also threat for banks, so it seems to be necessary to conduct relevant research on e-banking and the risks those could interfere with this system to identify the types of existing risks. Since, risk may have negative impacts on capital or bank revenues, the conceptual model of this research has been developed for applying the principles of crisis management to reduce the risks of electronic banking.

1.1. Electronic Banking and Risks

Electronic Banking is used to prepare any kind of access to banking services for customers through secure and convenient means without physical presence in the bank. Users of this system carry out financial operations without wasting time and expense in the bank [2]. Electronic banking branches include internet banking, mobile banking, telephone banking, ATM-based banking, e-banking, and bank card-based banking [3]. Risk on any kind of events is very important because it may have negative effects on capital and bank revenues [4]. Although, there are many risks in e-banking, most notably security risk, privacy risk, operational risk, reputational risk, legal risk and strategic risk, but the origin of risk comes from a lack of confidence that is always present throughout the life of the organization. So it is clear that the risk cannot be completely eliminated, but it can be reduced to prospect, or managed and guided properly. Since, the risk is uncertainly measurable [5], it is inherent in banking activities and virtually impossible to eliminate the risk of banking operations [6].

Security risk: Security risk is presented as unauthorized access to bank information such as the account system, risk management system, and so on. A breach of security can result in a direct loss of funds for the bank. For example, hackers can do business over the Internet, access and use confidential customer information, and virus replication. The result of this is the loss of information, theft or tampering with customer information, the disabling of an important part of the internal computer system of the bank, which leads to a violation of service and repair costs, etc. [7].

Privacy risk: Privacy comes back to the protection of personal information [8]. Privacy can be also defined as customer perception of the organization's ability to monitor and control customer information. One of the major obstacles on electronic trading is frustration and disappointment in the privacy of consumers. Consumers are concerned that the bank may place its customers profile as information and attempt to sell more products to other companies. In addition, the security and privacy of our customers are the most important challenges for the future of the bank. Maintaining personal information such as account numbers, passwords and transaction information is defined as the privacy of the customer. Failure to maintain this information is an important concern to e-banking. In fact, privacy in electronic banking is the ability of banks to monitor and control information in the customer's perspective. Sometimes, customers have a positive perception of giving information that banks are trusted [9, 10].

Operational risk: Operational risk as a trading risk is the most common type of risk associated with Internet banking. It results from inappropriate processing of transactions, non-performance of contracts, system failures, compromising data integrity, lack of privacy and confidentiality, unauthorized access, penetration into banking and transaction systems, and so on. These risks can be due to weaknesses in design, implementation, and monitoring of bank information systems. In addition to technological deficiencies, human factors such as negligence by customers and employees, fraudulent activities of employees, crackers and hackers can be a potential source of operational risk. There is often a subtle difference between operational risk and security risk, and both words are used instead [7].

Reputational risk: Internet allows quick information dissemination known as reputation or credit risk. Any incident is quickly reflected on the Internet and comes to the attention of many users or people. The speed of the Internet significantly reduces the response time not only for banks but also for users. Banks need to make sure that crisis management processes have the ability to deal with Internet related events. Reputational risk can occur when systems or products don’t securely work as expected, resulting in a widespread negative reaction. Reputation risk may also be created in cases where customers have not been given sufficient information about the use of the product. If there is a disturbance in access to the customer account, the bank faces a reputation risk. The risk of a hacker attacking the site and infiltration of its information also poses a risk to reputation. Risk of reputation does not threaten only a specific bank, but a threat to the entire banking system. If one of the banks faces a reputation risk, it also threatens the risk of other banks, and the general security of banking systems is questioned [11, 12].

Legal risk: There is a risk that arises from regulatory uncertainty in electronic money transfers due to the problem of identifying the location of an electronic company, called legal risk [11]. Due to the new nature of Internet banking, the rights and obligations are unclear in some cases and the use of unclear or obscure laws and regulations results in legal risk. Other reasons on legal risk are uncertainty about the validity of some agreements made through electronic media, customer rights, and privacy protections. A customer who is not adequately informed about the bank's rights and regulations may not have taken the necessary precautions in using Internet banking services and products, which could lead to problems in transactions, unexpected bank charges, or other common penalties [7].

Strategic Risk: This risk is related to the introduction of a new product or service in the electronic banking system. Misconceptions about the costs of developing operations or creating new operations, lack of adequate staffing staff to support operations are among the factors that contribute to this risk [13]. Electronic banking services should be consistent with the bank's financial strategy. A strategic vision should determine how to design, deploy, check, and control e-banking products. Bank officials should have an outlook for an e-banking program. Electronic banking requires strategic planning and evaluation by the management group as current banking services to expand into a new economic or geographic field. Planning and poor investment decisions in e-banking can increase the strategic risk of banks and financial institutions [7].

1.2. Crisis Management

The issue of crisis management has always been an important concern for organizations in competitive markets and for governments for disasters. A crisis, event, or incident is a natural, technical or social cause, with unforeseen consequences such as destruction or chaos. With increasing number and complexity of risks, this focus has been increasingly predicted to prepare for the coping phase in the crisis management cycle, and the efforts of governments and organizations to minimize the effects of these phenomena with the necessary measures. The well-known planning and crisis preparedness approach in the form of crisis management design is of great interest and attempts to reduce financial risks through preventive design [14, 15]. Crisis Management is defined as a systematic process in which the organization tries to identify and predict potential crises and then to take preventive measures against them in order to minimize their impact. As shown in figure 1, the three-stage model of the crisis management seems to be a comprehensive frame work. This model consists of three steps including before the crisis, during and after that. The pre-crisis phase includes all measures to prevent the crisis, the crisis stage, the steps to respond to and the response to the crisis and the post-crisis phase, including ensuring security of the organization and the organization's security and learning from the event in order to prevent its re-occurrence [16, 17].

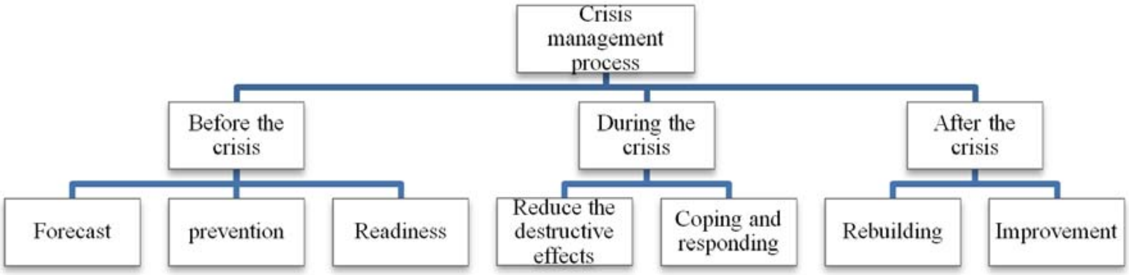

Figure 1. *Crisis Management Process.*

1.3. Vision

Electronic banking system is one of the essential tools for the realization and expansion of e-commerce and the use of electronic systems in financial and credit institutions is growing as well as the number of users of e-banking services is on the rise over the world. Since, this process is known as an opportunity and also threat for banks, so given the importance of the issue, it is essential that more research should be conducted on e-banking and the risks that could create a disruption to the system. Applying the principles of crisis management and identifying types of e-banking risks as effective solutions, which are the main viewpoints of this study, can be made to reduce them. Previous research works have identified e-banking risks and proposed methods to mitigate them in accordance with the recommendations of the Banking Supervision Committee.

In the present study, after explaining the most important risk components of electronic banking and finding ways to reduce these risks, the principles of crisis management are used to distinguish each of the risk reduction methods in the three stages before the occurrence of a risk crisis, during and after the occurrence. The relationships between the principles of crisis management and risk reduction methods have been investigated and which ways in which the risk reduction of e-banking is applied in each crisis management stage.

2. Research Methodology

In this research, e-banking risk components including security, privacy, operational, reputational, legal and strategic have been identified. Then, for each identified risk, methods and strategies for coping and reducing them are determined based on combination of principles crisis and risk management. By assessing and evaluating risk strategies, a conceptual model is presented based on the classification of risk reduction methods in which the risk domain and relevant associated strategies are presented. At the final stage, a questionnaire has been developed based on five point Likert Scale to assess the viewpoints of experts, managers and bank experts. The basis of the average review of the answers provided by the experts is compared to numerical average of 3 (μ=3) and finally the final conclusion is made. All research steps are now depicted in Figure 2.

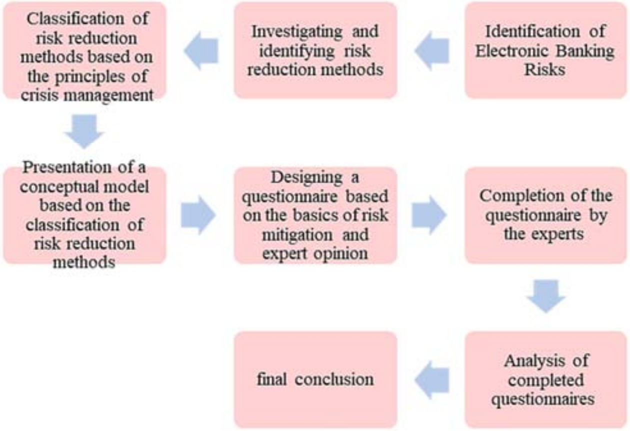
Identification of Electronic Banking Risks
Investigating and identifying risk reduction methods
Classification of risk reduction methods based on the principles of crisis management
Presentation of a conceptual model based on the classification of risk reduction methods
Designing a questionnaire based on the basics of risk mitigation and expert opinion
Completion of the questionnaire by the experts
Analysis of completed questionnaires
final conclusion

Figure 2. *The overall research process.*

3. Developing Conceptual Model

This model is presented after evaluating risk strategies based on the classification of risk reduction methods in which the risk domain and its associated strategies are presented. In this model, for each identified risk, risk reduction strategies are presented and classified into three steps of before, during and after the occurrence of risk. In the security risk that is presented as unauthorized access to essential bank information such as the account system, risk management system, etc., it includes fraudulent types of fraud and fraud committed through electronic communications and electronic banking. Before it happens, solutions such as the use of the SSL protocol and checking https at payment site, server authentication and the user, during the occurrence of this kind of risk from a strong firewall and anti-phishing, and after the occurrence, to manage the security risk crisis, change the code and password Internet are used. Principles of crisis management for operational risk in the pre-risk period are to improve the service quality and recruitment of skilled people in electronic banking. During the occurrence of risk, the monitoring system is used during data entry, processing, and withdrawal of information and after operational risk, the methods of payment of fines are used for the damage caused by making the wrong file and adding more security factors. All strategies for reducing each risk relevant to conceptual model of the present study are classified in Table 1. In this table, each suggestion is determined next to its code and the relevant cited reference, if referred.

Table 1. *Suggestions for Applying the Principles of Crisis Management to Reduce Electronic Banking Risks.*

Electronic Banking Risks	**Risk crisis management steps**		
	Before occurrence	**During the event**	**After occurrence**
Security risk	1. Use the SSL and HTTPS protocol [18] 2. Digital certificate 3. Server and user authentication [19] 4. Install anti-skimmer 5. Execution of ISMS 6. Execution of rules of PCI and DSS	7. Use antivirus and firewall 8. Use anti-spyware and anti-phishing [20] 9. Strong and expert IT staff	10. Block the attacker's or hacker's access by the firewall 11. change card password and internet password
Privacy risk	12. Use the SET protocol [21] 13. Informing about Electronic Banking Laws 14. Informing about the privacy of online banking customers	15. 16. Use antivirus and firewall implementation	16. Refer to the relevant branch and block the account 17. Tracking theft of information
Operational risk	18. Increase the quality of service SLA [22] 19. Teaching E-Banking Services staff 20. Hiring skilled people in e-banking 21. Development of ATMs, development of telecommunication networks, periodic review of individuals at key posts 22. Internal control, transaction tracking, licensing control for customers	23. Monitoring system for data entry, processing and data logging 24. Use of CCTV 25. Use of alarms such as prosecution of offenders	26. Fine for damages caused by making wrong file 27. Add more security factors 28. Gain experience and more financial strength
Reputational risk	29. Customer privacy 30. Informing customers about e-banking services 31. High security information 32. Increasing the Service Level Agreement	33. Increase in bank capital and financial strength	34. Receiving damages in the event of a bank's inability to meet its financial obligations
Legal risk	35. Transparency rules 36. Informing customers and employees 37. Formation of RRD [13]	38. Create restrictions, deprivations and heavy fines	39. Solving the ambiguities of laws and integrating them 40. Correction of Electronic Banking Laws
Strategic risk	41. Identify customer needs	42. Spending Opportunities Related to Assigning Capital to Electronic Banking	43. Creation of a group for examining the new electronic Service. 44. Creation of a group for future research.

4. Model Validation

One of the well-known ways to assess the validity of conceptual models is to conduct a questionnaire. The purpose of research based designed questionnaire design is to evaluate and validate each of the proposed solutions for risk reduction in electronic banking. The designed questionnaire which includes 28 questions related to risk reduction strategy, is based on the Likert scale of five choices filled out eventually by 38 experts, managers and others employees of state and private banks of Iranian northern province of Guilan. The basis for reviewing the average of the answers provided by the experts is compared to the use of the Likert scale with the mean number 3, and ultimately the final conclusion. The research designed questionnaire is shown in Appendix (A). As it can be observed, 28 statements are set up to assess the reliability of risk reduction strategies, so the well-known criterion of Cronbach's alpha coefficient is used to determine the approved and acceptable strategies using equation 1.

4.1. Questionnaire

After developing the conceptual model that includes crisis management stages and in each stage of risk management methods, in order to evaluate and validate the conceptual model, a questionnaire has been designed that each strategy as a question related to the risk reduction strategy in the questionnaire is inserted. For example, there is a type of risk known as security risk which can be managed in pre-crisis stage. It means that using SSL and HTTPS protocols can reduce the security risk in electronic banking. For validation of the proposed suggestion, one question has been designed as “The use of the SSL and HTTPS protocols at the Internet Banking Paid provides privacy protection”. Experts presented their opinions using Likert scale and data have been collected from all experts’ opinions to make a clear vote on proposing the above suggestion on is it suitable to apply or not. Other questions designed for all connections relevant to conceptual model in the questionnaire are shown in Appendix (1). The well-known measure coefficient of alpha

Cronbach is used for questionnaire validation calculated by equation (1), where, k is the number of questions, S_i^2 variance related to the answers to the question i from the question k and S_T^2 is the total variance of the questionnaire responses for each sample. If Alpha coefficient is more than 0.7 means that all questions are reliable to collect data for research purposes [23]. According to the Alpha coefficient, this questionnaire has a strong reliability. In this research, the Cronbach's alpha value was obtained with 28 statements 0.83. Following gathering all answers from completed questionnaires, the average and Variance value calculated for each column containing one proposition and 38 respondent samples.

$$\propto = \frac{k}{k-1}\left[1 - \frac{\sum_{i=1}^{k} S_i^2}{S_T^2}\right] \quad (1)$$

4.2. Checking Model Validation

A single-sample T test is based on a comparison with the mean and standard deviation performed on a small set of data. The T test is obtained by equation 2. Considering the fact that the 5-point Likert scale was used in the questionnaire, the basis for the examination and the value of the test item is μ=3 is considered, where, X is the mean value, μ is the basis of the survey, δ is the standard deviation and n is the sample number.

$$t = \frac{x-\mu}{\frac{\sigma}{\sqrt{n}}} \quad (2)$$

For testing and validation, T test value for one of the risk reduction strategies an evaluation of the solution for using the SSL and HTTPS protocols in an Internet Banking payment portal that protects privacy is done as follows: The solution was answered by 38 questionnaires with a mean value of 4.42 and a standard deviation of 0.59. The value of the variance is estimated to be 0.35 the value of the T-statistic is derived from the equation 2 of the number 14.63 and the significance level of zero is obtained. Since the numerical value is less than 0.05, the suggestion is accepted or approved. For other suggestions, the same way, the final result and the values obtained for each suggestion and results tabulated in Table 3. Results revealed that the proposed suggestions for risk reduction have been approved in the form of crisis management.

Table 2. *Suggestion for risk reduction.*

Code(s)	Suggestion for risk reduction approach
1	Privacy protection with SSL protocol on the Internet Payment Portal
1	Having the actual address of the bank's site to the https protocol to identify the bank's home site
2,3	Use multiple authentication like biometrics for more security at the time of transaction
4	Use anti-skimmer and install camera in ATMs
3	Notify alert via SMS or email and 2-step verification
16,17,23	Use of Intrusion Detection System by Banks for More Security
24,25	Use of alarms such as prosecution of offenders and Use of CCTV
5,6	Implementing ISMS Information Security System and enforcing PCI, DSS
7,10,15	The existence of a supervisory system in the bank and blocking the attacker's or hacker's access to the firewall
8	Use anti-spyware and anti-phishing to control fraud
11	Change the password of the card and the Internet after the occurrence of the risk
12	Secure credit card security by SET protocol
13,14	Information on e-banking rules and customer privacy in the Bank's quality policy
26	Considering the fine for damages caused by making a wrong file by a bank employee
27,28,33	Add more security factors and gain more experience and financial strength
9,19,20	Training for e-banking services staff and recruiting skilled people in e-banking
18,32	Guaranteed service quality parameters by increasing service quality guarantee (SLA)
28,29	Privacy e-banking customers
21	Development of ATMs, development of telecommunication networks, periodic review of individuals at key posts
22	Internal control, transaction tracking, licensing control for customers
36	Identification of information security policies for all personnel in banking systems
34	Receiving damages for customers in the event of the bank's inability to meet its financial obligations
37	Transparency of rules, formation of a reference base of RRD rules, resolution of ambiguities and amendments to e-banking rules
38	Create restrictions, deprivations and heavy fines
30,31	Providing high level of information and giving customers complete information about e-banking services
35,39	Hiding the terms and conditions of the banks, the rights of obligations between the organizations and customers
41,42	Identifying customer needs and the adequacy of information management systems to track the performance and profitability of e-banking
40,43,44	Changing rules and regulations with respect to e-banking capacities and creating a group to review new e-services

Table 3. *T-test results for all filled out questionnaires.*

Suggestion Code(s)	Mean	Standard deviation	Variance	(T-stat)	(p-value)
1	4.42	0.59	0.35	14.63	≈ 0
1	4.42	0.64	0.41	13.63	≈ 0
2,3	4.76	0.43	0.18	25.22	≈ 0
4	4.68	0.47	0.22	22.04	≈ 0
3	4.60	0.54	0.29	18.08	≈ 0
16,17,23	4.07	0.63	0.39	10.52	≈ 0

Suggestion Code(s)	Mean	Standard deviation	Variance	(T-stat)	(p-value)
24,25	4.23	0.75	0.56	10.15	≈ 0
5,6	4.34	0.62	0.39	13.19	≈ 0
7,10,15	4.36	0.75	0.56	11.23	≈ 0
8	3.21	0.99	0.98	1.31	0.09
11	3.86	1.11	1.25	4.78	≈ 0
12	4.07	0.71	0.50	9.34	≈ 0
13,14	3.63	0.71	0.50	5.45	≈ 0
26	3.36	1.12	1.26	2.01	0.02
27,28,33	3.89	1.10	1.23	4.96	≈ 0
9,19,20	3.63	1.17	1.37	3.32	0.001
18,32	3.63	1.12	1.26	3.46	0.0007
28,29	4.86	0.34	0.11	33.62	≈ 0
21	4.57	0.55	0.30	17.64	≈ 0
22	4.15	0.85	0.73	8.34	≈ 0
36	3.84	1	1	5.18	≈ 0
34	3.42	1.10	1.22	2.34	0.01
37	4	0.82	0.68	7.24	≈ 0
38	3.56	1.14	1.30	3.01	0.002
30,31	4.02	0.82	0.67	7.70	≈ 0
35,39	2.92	1.44	2.07	-0.34	0.18
41,42	4.39	0.59	0.35	14.46	≈ 0
40,43,44	4.34	0.84	0.71	9.76	≈ 0

Considering the 95% of confidence interval, suggestions with p-value of more than 0.05 have not been approved. So, according to Table 3, the solutions “Use anti-spyware and anti-phishing to control fraud” and “Hiding the terms and conditions of the banks, the rights of obligations between the organizations and customers” have not been approved and other suggestions can be considered to reduce the risk in e-banking activities.

5. Summary and Conclusion

In this research, risk reduction methods have been investigated on electronic banking. Following a proposed conceptual model, each suggestion for risk reduction is adapted based on the principles of crisis management, which includes the pre-crisis stage, during the risk crisis and after that. For each risk a suggestion is considered which should be applied to reduce the correspondent risk. In order to check the validity of conceptual model, a questionnaire has been designed in which each strategy as a proposition related to the risk reduction step is connected to a specific question. Conceptual model has been validated after gathering the data from questionnaires filled out by experts, managers and banking staff. Statistical analysis was performed utilizing T-test in which for each of the risk-related suggestion, the T-test and the significance level have been calculated, and the correspondent suggestion is approved if the significant level is smaller than 0.05. In general, results goes to have a positive attitude towards the proposed risk reduction strategies, means that risk can be more managed over the e-banking activities. For further studies in this field researchers are recommended to study more on the below headlines:

a) This model provides risk mitigation strategies in e-banking according to the principles of crisis management. It is possible to check suggestions related to customers and e-banking staff in two distinct parts as a new conceptual model.

b) Each suggestion presented in the conceptual model of research may be a costly activity for both organization and bank. It is recommended to investigate suggestions considering operation costs of suggestions.

Appendix: Questionnaire

This questionnaire is designed to assess the security status of electronic banking systems and e-banking risk reduction methods in Internet, mobile, Internet-based payment portals, ATM terminals, and e-commerce card readers. For each of the risks of e-banking, risk reduction strategies are presented in the following questionnaire as a proposition related to the risk reduction strategy. By filling out the questionnaire by experts, senior executives, employees and banking experts, each of the solutions is validated.

Appendix A. *Questionnaire designed to validate conceptual model using Likert five-scale rates.*

Code(s)	Question associated with the risk reduction strategy	Quite agree	Agree	Somewhat	Disagree	Totally disagree
1	The use of the SSL and HTTPS protocols at the Internet Banking Paid provides privacy protection.					
1	To identify a bank's primary site and a fraudulent site, the actual address of the bank's site in the browser's address bar must be HTTPS.					
2, 3	Using multiple authentication (such as passwords, biometric methods, such as electronic signatures or fingerprints) makes more security when entering and doing transactions.					
4	To reduce the risk of ATMs, anti-skimming and camera installation are effective.					

Code(s)	Question associated with the risk reduction strategy	Quite agree	Agree	Somewhat	Disagree	Totally disagree
3	To authenticate the e-banking user, alert via SMS or e-mail, and two-step verification during the transaction is necessary.					
16, 17, 23	Banks use intrusion detection systems and identify unauthorized activities for greater security.					
24, 25	Banks use logging and event logging systems and systematically inspect information to discover suspicious transactions.					
5,6	Implementing the ISMS Information Security System to secure the data exchange environment in banks and enforce PCI rules, DSS is essential for the security of payment cards.					
7, 10, 15	For data entry, processing and deletion of information in the bank, there is a monitoring system and access to the attacker or hacker is blocked by the firewall.					
8	Anti-spyware and Anti-phishing are not very effective in preventing and controlling phishing scams (fake sites).					
11	After the occurrence of risk, changing the password of the card and the Internet code does not have an effect on reducing the risk of electronic banking.					
12	The secure credit card security SET protocol ensures that the order information is securely transmitted between the different parts over the Internet.					
13, 14	Information about e-banking rules and the privacy of online banking customers is announced in the Bank's quality policy.					
26	For losses caused by making a wrong file by a bank employee, it's best to consider a fine.					
27, 28, 33	After the risk, adding more security factors and gaining more experience and financial power will be useless.					
9, 19, 20	E-banking staffs are given training and skilled people are hired in e-banking.					
18, 32	Increasing Service Quality Guarantee (SLA), a legal contract between the service provider and the service provider, is not affected by the reduction of electronic banking risk to ensure quality service parameters.					
28, 29	Privacy safeguards customers' confidence in e-banking. Maintaining personal information such as account numbers, ciphers and transaction information is part of the customer's privacy.					
21	The development of ATMs, the development of telecommunications networks, the level of technology used in credit cards, periodic reviews of individuals in key posts, the classification of sensitive data and limited access of employees to reduce the operational risk of electronic banking.					
22	Internal control, the ability to track transactions, control the opening, change and close an account by the customer, and control the issuance of permission to enter customers into the electronic banking system (credential validation) has little effect on the reduction of operational risk.					
36	It is not necessary to identify information security policies for all personnel in banking systems.					
34	From risk reduction strategies, there is a possibility for customers to receive damages if they are unable to meet their financial obligations.					
37	The transparency of the rules, the creation of a reference base for RRD rules, the resolution of ambiguities, and the revision of the laws related to electronic banking, are not considered as risk reduction methods for e-banking.					
38	In order to protect banks against reputational, legal and commercial risks, electronic banking services should not be performed on a regular basis in accordance with customer expectations.					
30, 31	To reduce the risk of e-banking, things like high information security, customer privacy, and full customer information about e-banking services are being used.					
35,3 9	To avoid legal issues, banks need to hide the terms and conditions, related rights, and obligations between their organizations and their customers who use e-banking.					
41, 42	Identifying customer needs and the adequacy of information management systems to track the function and profitability of e-banking is one of the appropriate strategies before the occurrence of risk.					
40, 43, 44	After the occurrence of risk, changes to the laws and regulations affect the capacity of electronic banking and the creation of a group for the investigation of new electronic services.					

References

[1] Abdou, H., English, J. & Adewunmi, P. (2014), ‘An investigation of risk management practices in electronic banking: the case of the UK banks’, *Banks and Bank Systems, 9* (3). pp. 19-31. ISSN 1816-7403.

[2] Abbasi Aabkhare, A., Mahmoud Alilo, B., & Abedini, E., (2013), Advantages and Disadvantages of E-Banking and Commerce, *Life Science Journal*, 10 (4s), pp. 458-462.

[3] Safarpour, M., (2016), Identification and ranking the barriers to adoption and development of electronic banking in Iran. *1st International Conference on Applied Economics and Business, Procedia Economics and Finance, vol. 36,* 374-380.

[4] Cobb, S. (1996), “*Security Issues in Internet Commerce*”, Proc. IEEE.

[5] Torrubia, A., Mora, F. J., Marti, L. (2001), “Cryptography Regulations for E-commerce and Digital Rights Management”, Computers & Security Vol. 20, No. 8, 730-731.

[6] Liao, R., Kishore, R. (2017), “Trust and Risk in E-Commerce: A Re-examination and Theoretical Integration”, *SIGMIS-CPR'17 Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research, Pages 61-62, Bangalore, India.*

[7] Zarei, Sh. (2011),“Risk Management of Internet Banking”, *International Conference on Artificial Intelligence, Knowledge Engineering and Data Bases. Cambridge, UK - February 20 - 22, 2011, pp. 134-139.*

[8] Manzano, A., Joaquı´n and Lassala-Navarre´. Carlos and Ruiz-Mafe´. Carla and Sanz-Blas. Silvia, (2009), “The role of consumer innovativeness and perceived risk in online banking usage,” *International Journal of Bank Marketing,* Vol. 27 No. 1, pp. 53-75.

[9] Yousafzai, S. Y., Pallister, J. G., &Foxall, G. R., (2003). A proposed model of e-trust for electronic banking. TECH Technovation, 23 (11), 847-860.

[10] Hoffman, D. L., Novak, T. P. & Peralta, M. A., (1999) Building consumer trust online. Communications of the ACM, 42 (4), 80–85.

[11] Al-Smadi M., Al-wabel S. A. (2010). E-Banking on of Jordanian Banks; Journal of Internet Banking and Commerce, Vol. 14, No. 1, pp. 1-10.

[12] Tattam, D. (2017).*Reputation Risk: Risk Event or Risk Consequence?*Protect Risk Management Insights. *Retrieved 2017-05-01.*

[13] Khezri, R. &Tavallaei, R. (2014). Risk Management Strategies of Electronic Services in the Iran’s Banking System. *International Journal of Innovation, Management and Technology, Vol. 5, No. 5, pp. 351-357.*

[14] Perry, R. W., Quarantelli, E. L., (2004), what is a Disaster? More Perspectives. Philadelphia, Xlibris.

[15] Alexander, D. (2002). From civil defense to civil protection-and back again. Disaster Prevention and Management, vol. 11, no. 3, 209-213.

[16] Campion, M. A., Medsker, G. J and. Higgs, A. C. (1993). Relations between work group characteristics and effectiveness: Implications for designing effective work groups. Personnel psychology, vol. 46, no. 4, 823-847.

[17] Pagell, M and LePine, J, A. (2002). Multiple case studies of team effectiveness in manufacturing organizations. Journal of Operations Management, vol 20, no. 5, 619-639.

[18] Clark, j. Oorschot, p. (2013). SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. *IEEE Symposium on Security and Privacy. 511-523.*

[19] Amtul, Fatima. (2011). E-Banking Security Issues – Is There A Solution in Biometrics?. *Journal of Internet Banking and Commerce*, August 2011, vol. 16, no. 2. pp. 1-9.

[20] Shekokar, N. M., Shah, Ch., Mahajan, M. & Rachh, Sh. (2015), An Ideal Approach for Detection and Prevention of Phishing Attacks. *Computer Science 49, 82-91.*

[21] Elkamchouchi, H., Abu Elkhair, E., Abouelseoud, Y. (2013). AN IMPROVEMENT TO THE SET ROTOCOL BASED ON SIGNCRYPTION. *International Journal on Cryptography and Information Security (IJCIS), Vol. 3, No. 2, 1-13.*

[22] Anithakumari, S., Chandrasekaran, K., (2015), “Monitoring and Management of Service Level Agreements in Cloud Computing’, *International Conference on Cloud and Autonomic Computing. IEEE 2015, pp. 204-207.*

[23] Cronbach LJ. (1970). Essentials of Psychological Testing. Harper &Row, 3rd ed., New York, Harper and Row Publishers.

Biography

Maedeh BabaeiChafjiri: received Bachelor of Science in Software Engineering from PNU university of Astaneh-Ashrafiye. She receiveda Master of Engineeringdegree in IT and E-commerce from Mehrastan University in Guilan, Iran. She is one active member of young researcher club in Islamic Azad University, the branches of Roudsar and Amlash. Her main research interests include E-commerce, Risks of E-banking, and Security in E-banking and mobile banking, Secure web. She teaches some courses on computer for ten years.

Abbas Mahmoudabadi, is faculty member at MehrAstan University, Guilan, Iran. He received Ph.D. degree in January 2014 in the field of optimization in Hazmat transportation and received Thesis Dissertation Award from IEOM society in 2015. He has published near 75 journal or international conference papers published in the field of industrial engineering, transportation and traffic safety and e-commerce. He teaches transport and industrial engineering courses and has around 26 years of experiences on traffic and road safety planning in developing countries. He has also strong cooperation with national and international agencies on traffic safety and industrial engineering.