MODERN APPROACHES AND CHALLENGES OF RISK MANAGEMENT IN ELECTRONIC BANKING

Dr Dragan Stojanović[1]; M.Sc. Marko Krstić[2].
[1] Higher Business School, Leskovac, SERBIA, e-mail: stojanovic.dragan@vpsle.edu.rs
[2] Higher Business School, Leskovac, SERBIA, e-mail: krstic.marko@vpsle.edu.rs

Abstrakt: *The development of a new form of banking, known as electronic banking, is the result of a growing need of the use of communication-information technology. Electronic banking is known for its numerous advantages such as reduction of time in the execution of financial transactions, increase in the efficiency of business operations, reduction of business costs, etc. In addition to the numerous positive effects of development of electronic banking, we must consider the fact that it is precisely this new way of performing financial transactions that has lead to an appearance of ever greater number of new risks. The specifics of risk in electronic banking stems from the specific ways of performing financial transactions online using smart cards, ATMs, smart phones etc., and the possibility of misuse with this form of performing business transactions. Having this in mind, the aim of this paper is to point out the risks of electronic banking which both banks and their clients face all the while placing special attention on examples of risk management of electronic banking.*

Keywords:*Electronic banking, financial transactions, risk management in electronic banking, communication-information technology.*

1. INTRODUCTION

Development of modern technology brings about the application of new ways of performing business operations in all areas, i.e. areas such as production, trade, tourism and financial operations. Moreover, the growing competitiveness and the process of globalization of financial market have made banks (being the most important financial institutions) obvious examples of inevitability of application of modern information-communication technology with the aim of preserving their position on the financial market. Therefore, it is necessary to place special attention on electronic banking as an innovative way of banks' operations which is gaining in importance.
The very specifics of electronic banking stem from the fact, that, although, it brings numerous benefits in the operations of banks, these specifics also lead to creation of new types of risks and their intensification.Having this in mind, in what follows, special attention will be placed on the role and benefits which the modern information-communication technology offers to banks through the prism of electronic banking, as well as its characteristics and further tendencies in development. We will also discuss different types of risks which stand as an obstacle to a more intense development of electronic banking as well as information-communication technology and its advantages when it comes to managing various risks that can appear in electronic operations of banks. Finally, we present examples of ways of risk management in electronic banking.

2. ELECTRONIC BANKING AND ITS CHARACTERISTICS

Intensification of use of modern information-communication technology and the Internet, has led to a change – namely, traditional ways of performing banking operations have been replaced with an innovative way which is based on electronic operations. Thus, electronic banking has become a dominant way of performing almost all financial transactions and a great source of income, on one hand, and a powerful tool in terms of competitiveness, on the other hand. [14]
Electronic banking represents a possibility of providing financial services to clients of the bank (which can be either a natural person or a legal person) using the Internet, ITMs, wireless networks and other electronic devices. It includes online banking which refers to provision of financial services to clients over the Internet (using computers or mobile devices), mobile payments over wireless networks, self-service terminals like ATMs as well as mobile banking which refers to the use of both regular and mobile telephone networks.[7]

Moreover, electronic banking represents automatic delivery of new and traditional banking products and services using electronic channels, computers and telecommunication equipment. Electronic banking can be said to represent one of the most important surrounding aspects in the e-business itself and electronic trade.[8]

2.1. Advantages of electronic banking

Besides providing more efficient day-to-day services to clients of banks, electronic banking is linked to numerous advantages such as the speed of performing financial transactions with payments or transfer of funds, a simpler use thanks to detailed instructions, decrease in business costs of banks, increase in client satisfaction and with it increase in the number of users of electronic banking.[8]

Numerous factors affected the rapid acceptance and implementation of electronic banking method and the increase in the number of users of electronic banking. Some of those factors are:[5]

- **Price efficiency** where the use of modern information communication technology and the Internet led to a decrease in administrative costs and time necessary to perform certain transactions. This entails an increase in the speed of performing these transactions. On this occasion, it is important which channels of electronic exchange of data are used, as well as the fact that it is necessary to consider both decisions which refer to costs of further development and introduction of innovations in the e-banking field, costs of marketing and costs of maintenance of the entire system.
- **Growing competitiveness in provision of financial services** where banks, by implementing electronic banking, differentiate themselves in relation to other financial institutions and thus retain the existing client and attract new precisely with the advantages the new system provides.
- **Globalization of business operations** where bank clients are able to use the electronic banking services using Internet connection from any location, without any time limit as well as providing banks with an opportunity to be involved on the financial market on a global level, without the need to open branch offices.
- **Demographic characteristics of bank clients**. Bearing in mind clients' diversity in terms of age, gender, education, etc., it is necessary to point out the fact that electronic banking offers its clients different types of services. Some clients will be interested in using services that can be performed on bank counters while other clients will want to use the most advanced, innovative services such as paying their bills using their smart phones, etc.
- **Obtaining more clients through branding of services of electronic banking.** E-banking services that one bank provides, and which are unique in relation to the services of other banks, can very much develop and preserve good business relations with the existing clients. In such situations, clients, through the feeling of using branded services, become loyal to a particular bank which allows this bank to attract an even bigger number of clients and ultimately increase its profitability.

Besides these, some other advantages of electronic banking are related to a more successful adaptation to the ever changing clients' needs, considering the possibility of sending momentary feedback on clients' satisfaction with a particular service. Furthermore, implementation of electronic banking brings a decrease in the amount of paperwork and consequently, decrease in the number of possible errors bank employees' can make. This can be one of the reasons a great amount of people accepts the opportunities electronic banking offers. Of course, we must mention the possibility of performing a greater number of banking services (where clients do not have to go to banks to perform some banking service) using computers, using certain banking applications of electronic banking as well as using the services of mobile banking with appropriate smartphones.[8]

3. RISKS OF ELECTRONIC BANKING

Besides its numerous advantages, electronic banking is based on the use of modern information-communication technology and the Internet. As such, it has opened a way to a more intense exposure to the existing risks, on one hand, and to the emergence of new risks, on the other.[13]

Some of the most important risks related to electronic banking are: [5]

- Credit risk;
- Risk of interest risk change;
- Liquidity risk;
- Price risk;
- Transactions risks, etc.

In addition, we can mention some other risks such as: [11]

- Risk of compliance with legal regulations;
- Reputation risk, and
- Risks related to security of information.

One of the most important risks of electronic banking is the transaction risk. The transaction risk represents a current and a potential risk which may lead to a decrease in profit and capital of a bank. This risk arises from the possibility of occurrence of immoral actions of bank's employees in bank's business operations, i.e. frauds, mistakes and an inability to extend the required services to bank's clients or perform banking operations. It also refers to mistakes within the system of transfer of funds, development of computer systems and software solutions, internal control measures, etc.[5] Some other risks of electronic banking are the question of security which creates a gap between a bank and its clients in terms of mistrust in using new technology on which electronic banking is based, as well as complex operative and technological barriers. Namely, every client expects its bank to provide a safe information systems whose use will not lead to any kind of loss of information and which will enable its clients to obtain the service they requested without any delay in its execution. If a system of electronic banking was not in line with clients' expectations and if it could not be trusted in terms of its reliability, speed and accuracy and if there existed a possibility of misuse of information by hackers, such situations would lead to a decrease in electronic banking consumer satisfaction. Ultimately, this would mean losing clients. With this said, it is important to understand which side (benefits of electronic banking or risks related with its use) has greater impact on clients' satisfaction. This question was answered by a research conducted by Jehangir, Zahid, Jan, and Khan,who surveyed 201 users of electronic services with 5 commercial banks in one district in Pakistan. The researchers used Likert's scale. A total of 33 questions was divided in four categories where 4 questions referred to demographics, 10 to client satisfaction, 9 to advantages of using IT in electronic banking, and 10 questions referred to risks related to IT. By processing data and analysing them using SPSS 16.0 and Microsoft Excel 2011, they came to the conclusion that e-banking brings many advantages to banks thus enabling them to preserve their competitiveness. In addition, there are many risks that must be considered when formulating business strategies of each bank. Implemented IT systems must make electronic banking much safer and reliable for clients' use. This research confirms the researchers' hypotheses that the advantages of electronic banking have a far greater influence on clients' satisfaction then risks related to electronic banking which in turn cause clients' dissatisfaction with banks included in the research. [8]
The following image confirms the importance of preserving the safety and protecting data of those clients of a bank using the services of electronic banking which will in turn lead to increase in user satisfaction. The image presents the losses caused by committed frauds in online banking in Great Britain for the period from 2010. to 2015. (amounts are presented in millions).

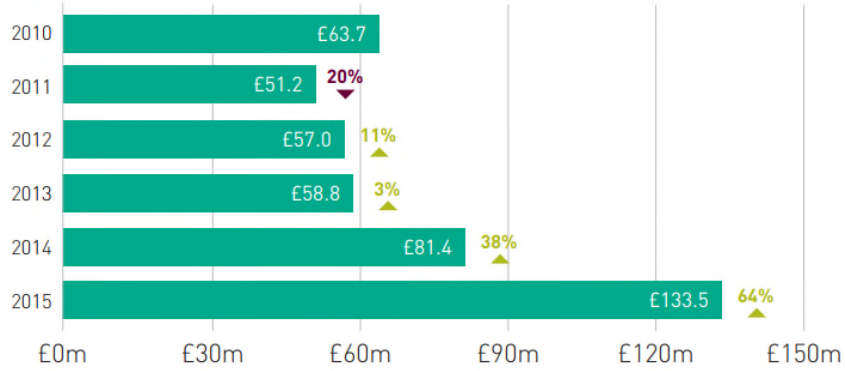

Figure 1: The amount of losses as a result of financial frauds in online bankingin the UK, and the percentage of change in relation to previous years in the period from 2010 to 2015 in millions of £ [4]

It is believed that different factors contributed to an increase in the number of frauds in the area of e-banking, the dominant ones being phishing, vishing (phishing using a telephone) together with malware attacks.[4]As banks and their clients are exposed to different types of risk which are gaining in importance if one considers their impact in relation to losses they can cause and considering the rise of new types of risk, in what follows, the paper deals with risk management in electronic banking and offers examples to understand ways of managing different types of risks.

4. RISK MANAGEMENT IN ELECTRONIC BANKING

Continuous technological innovations and competitiveness amongst banking organizations and new participants on the financial market have increased the level of accessibility of different banking products and services to their clients through electronic banking. However, the fast development of this type of service has made it much more possible for various risks to appear which in turn can have devastating consequences on the entire financial system. This is why it is extremely important for each financial institution to implement (as part of its business strategy) and apply a particular process of management of technology risks where risk management represents a process of risk identification and

taking certain steps to ensure confidentiality, integrity and availability of all components in the information system of an organization. This would enable the monitored financial institutions to carry out adequate measurement, monitoring and control of exposure to certain types of risks.[5]

The importance of introducing an adequate system of risk management in banks is confirmed with the fact that there is a great amount of conditions prescribed by both regulatory and supervisory bodies, such as conditions stipulated in the Basel agreement. Besides this, it is important to stress the fact that modern information-communication technology, which represents the very basis to the system of electronic banking, should, in great extent, contribute and be a foundation to a more efficient risk management process, based on continuous development and system adjustments. [13]
Banks that conduct their business operations beyond the boundaries of a country in which they were established and perform transactions on an international level, must bear in mind that there exists a need for a process to successfully perform transactions between banks, their clients and foreign business partners. Besides the possibility of occurrence of transaction risk, this is when other risks (such as reputation risk, credit risk and liquidity risk) on the basis of non-executed transactions can occur.
This is why banks have developed and implemented in their systems of business operations, different information-communication technology in order to successfully manage these types of risks. When it comes to big amounts which are being transferred from one account to another, it is necessary to point out that one of the most important facts for business operations of a bank is the safety of performing such transactions which is achieved through protection of the identity of the clients and their personal data.[5]
Thus implementation of innovative technology can lead to creation of risks as well as it offers great possibilities in the matter of risk management. The fact is that constant changes in the application of modern technology imposes a need to monitor the existing risks but there is also a need to monitor the emergence of new types of risk and to continuously adjust methods of risk management by applying and improving this innovative technology.[13]
Regarding the principles of risk management in electronic banking, they can be divided into three categories which are: [9]

- **Board and management supervision** which is used to achieve adequate analysis, monitoring and control of activities in electronic banking which refer to risk management where these activities must be fully implemented within the framework of the overall strategy of bank's operations.
- **Security control** where it is particularly important to create a data base which will contain data on performed transactions via electronic banking and their entire records. Moreover, it is important to mention the issue of confidentiality of information about banks, proper control of authorization within electronic banking system, authorization of clients using the services within the system of electronic banking, etc.
- **Management of legal and reputation risks** which refer to requirement set to banks in relation to achieving a certain level of trust and safety with provision of services of electronic banking and protection of all clients' data from misuse.

5. EXAMPLE OF RISK MANAGEMENT IN ELECTRONIC BANKING

5.1. Risk management in electronic banking using biometric methods and preventive measures

Given that transaction risk can have unimaginable consequences on the operations of each financial institution, it is necessary to indicate which ways it is possible to manage this type of risk. One of the ways is the use of biometric technology which is used for client identification prior to payment of certain amount of money.[5]
With biometric technology we should consider and evaluate the characteristics such as universality in the sense that each person possesses personal, unique characteristics, which differentiate him/her from others, a uniqueness where there are no two people with identical characteristics, and tenability which implies that these characteristics do not change over time, with the exception of the face. Moreover, these characteristics must be easily determined with technology which gives accurate results under different circumstances. Namely, this technology determines the characteristics of a particular face and acceptability of methods under which the required characteristics are determined (the technology cannot be fooled in any way possible). [5]
There are two biometric technology methods which are used with verification and identification and these are: behavioral biometrics and physical biometrics. Behavioral biometrics refers to verification and identification of voice, signature, etc., while physical biometrics refers to verification of fingerprints, face recognition, geometry of hand form, analysis of retina, etc.[5]
In order to prevent fraudulent activities and illegal incursion in electronic banking system i.e. prevent the possibility of hacking and downloading huge amounts of money from clients' accounts, it is recommended to use general architecture as part of technological solution which enables detection of fraudulent activities and their momentary prevention. It includes identification of devices which are used to access the account within the framework of electronic banking

services by using a component which must be downloaded and must be installed on the client's device. This component generates the so called imprint on the client's access device and this can be a serial number which is set to bank's website with every transaction. Besides this, it is important to monitor the client's behavior on a global level, where, if it is noticed that a client is using different access accounts and accesses his/her account from different devices, this can be perceived as the first sign of a possible threat. It is also important to perform a global analysis and formulate three lists, where the first represents a black list of identities which are seen as a serious threat, the second one, white list, containing legitimate identities and the third list, a list of suspects which are not classified in any of the previously mentioned categories. Exponential decay function is performed to determine the probability of fraud committed by the user of a device which is included in the list of suspects. If any fraudulent activity is noticed, the device used to perform such activity is automatically placed on the black list.[1]
However, besides these, there are safety measures which are used to ban unauthorized access to a bank account and thus prevent frauds. Namely, the approach used in this case is made of 5 steps where the user first inputs an access code, the so called ID number. Then the user enters his password after which the user has to answer question whether he/she wants additional safety measures to be applied on his/her account. The client then enters additional personal information and what follows is the fifth step which includes identification of a specific image (the image is previously selected by the user). It is then possible to perform all services offered by the electronic banking system. [1]

5.2. Improvement of information support to the process of risk management through implementation of information system – example of Ukrainian banks

The introduction of information system which will enable support to the process of risk management in electronic banking in banks is of extreme importance and its implementation is in accordance with business objectives. This enables implementation of information system in banks within 3 organizational levels.[2]
This way of doing business enables the most efficient exchange of information between management levels and offers solutions to achieving goals of banking operations. Exchange of information is of key importance when it comes to the monitoring of achievement of business goals and risks that any bank faces starting from the highest level of management to the lowest with simultaneous participation of experts in the field of risk management, analysts and others, which can be seen in figure 2.[2]

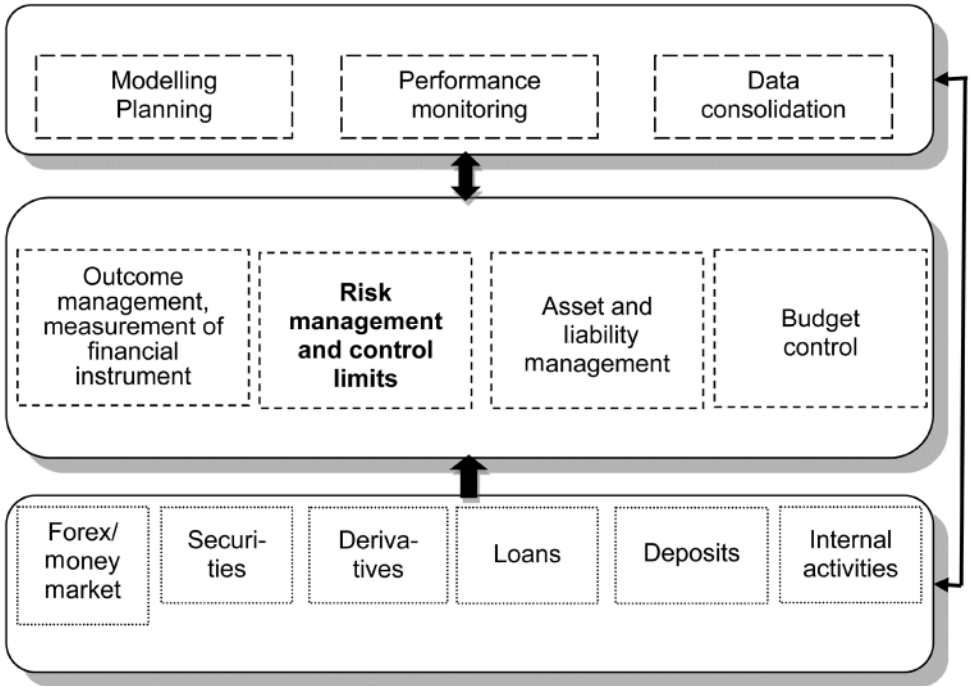

Figure 2: Three levels of banks' information management system[2]

This type of system structure enables complete transparency of data and cost control. The highest level represents strategic management which includes making of plans, performance measurement and data consolidation after which, analysts at the middle level of management get specific tasks in the form of tables and concrete indicators set as goals. Other activities performed on the middle level are calculations of numerous sizes, among which there is the determination of the probability of occurrence of a certain risk as well as the amount of damage that it may cause. This

enables provision of information related to the rate of return of bank's funds and transaction risk to the lowest operative level where activities on the monetary market are performed. These include issuing of bonds, loan approval, deposit collection, etc. The given example testifies to the importance of risk management process bearing in mind that it represents a link between the highest and the lowest level in a financial organization and the center of total activity of a bank. [2]

5.3. Risk management in electronic banking on the example of Continental national bank from Miami

The importance of adequate process of risk management related to electronic banking is evidenced by client recommendations from Continental national bank (whose headquarters are in Miami). These recommendations refer to appropriate application of identification number and password while the measures for adequate account protection include constant password change, avoidance of using personal information or numbers to create passwords, avoidance of password saving on computers, etc. Besides this, another recommendation is to always access one's account from a personal computer and not from a public computer and to check your account balance every day. It is not recommended to perform transfers online if you have several windows opened in the Internet browser you are using. There is also a possibility of setting up different types of system alarms which are triggered once an unauthorized activity takes place (these include alarms that signal the change of password, alarms that signal transfer of money, etc.)[3]
An efficient way of managing transaction risks and data is to use the option of setting up limits for money transfer from one account to another. When it comes to protection from software viruses, it is necessary to avoid opening mails from unknown sources, giving personal information, user name, PIN code or passwords over e-mails, even if they were sent via known source. Moreover, installing and regular updating of an anti-virus software can, very much, prevent the occurrence of operative risks in banks. A more efficient risk management in electronic banking requires installing a network security system (firewall) to prevent unauthorized access to clients' bank accounts.[3]

5.4. Risk management in electronic banking on the example of Indian banks

Discussing the banking system in India, we can say that the introduction of electronic banking has lead to great transformations in the very way of execution of banking operations and that the number of users of ATM machines, online banking, mobile banking, telephone banking, credit and debit cards is constantly increasing.[10]However, considering the numerous risks which are related to electronic banking (such as frauds related to unauthorized use of credit and debit cards, identity theft, use of software viruses or system hacking, etc.), it is important to point out the efforts made by the Reserve Bank of India (RBI) to implement measures for an efficient risk management in electronic banking, with the aim of preserving security of such transactions.[12]
In this case, special attention is placed on: [12]
1. Safety and technology related issues; When it comes to standards relating to technology and security, banks should create a network and data base administrator which would enable the use of the latest version of a licensed software by authorized groups of users which have access to the given system. Each bank should have its own security business policy approved by the Bank's Board of Directors. Banks should also use logical control of data and system access by using user names, passwords or other biometric methods. No bank should allow a direct connection between the Internet and the system of electronic banking itself, which is achieved through the use of adequate firewall. Banks should also use PKI (Public Key Infrastructure) which ensures the safety of provided services of electronic banking. It is also recommended that all unnecessary services on the server, such as FTP (File Transfer Protocol) be disabled. It is important to install, within the framework of the system, tools which would monitor and reveal attempts of unauthorized system access, as well as different types of software alarms. All bank's applications should be able to store all data and messages in a deciphered and readable form and they should take into account that it is necessary to test the security infrastructure prior to its implementation. Of course, it is important to perform regular software updates. The information security officer and information system auditor should perform periodical systems tests which include attempts to compromise passwords using certain hacking tools, attempts of system overload using DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks, control of software adequacy where it is recommended to consult external experts with the execution of this control.
2. Regulatory issues; Considering the legal position, banks are required, not only to determine identity, but to consider the integrity and reputation of a potential client. Moreover, from a legal point of view, safety procedure that banks adopt of user authentication have to be recognized by the law, as a form of substitution for the electronic banking user's signature. Since the legal obligation of banks in relation to maintenance of confidentiality and secrecy of information about their clients, banks have to develop adequate systems of risk management in order to meet this requirement. With regard to online banking, banks should clearly inform their clients of the timeframe and circumstances in which it would be possible to accept any order in relation to the termination of the process of transfer of money from one account to another. Consumer rights which are defined under the Consumer protection Act in India also refer to protection of rights of bank clients (those using electronic banking services) and to the identification of rights and responsibility in relation to emergence of risks in electronic banking and their negative consequences for clients.

3. Supervision and operation issues. It is important to point out that only licenced banks with work permits (issued by the monetary authority) whose headquarters are located in India, can offer electronic banking services to residents of India (in domestic currency). After formulating their business plan, cost-profit analysis and adoption of standards referring to the use of technology and risk management process, together with the security policy related to e-operations, banks must submit a request to the Reserve Bank of India to obtain an e-banking work permit. Furthermore, banks have an obligation to report any failure in the security system and any loss occurring as a consequence of such event. Banks must adhere to instructions provided by the Reserve Bank of India which refer to risks and control of computer and telecommunication systems, where all risks related to electronic banking will be covered as part of regular inspection analysis. Banks have to develop outsourcing guidelines in order to efficiently manage risks which are associated with services provided by external business partners. With the increasing popularity of e-trade, it has become necessary to develop Inter-bank Payment Gateways with the purpose of settling such transactions. The connection between two computer systems between different banks and clients should be enabled by using separate, leased networks, not the Internet. This is, of course, performed with adherence to certain standards for data encryption. Banks must disclose risks, client's responsibilities and obligations which refer to electronic banking through certain reports all the while enabling certain transparency of its financial reports. Banks also have to efficiently manage the reputation risk taking into account which advertising messages (directed towards users of electronic banking services) they can air on their web page.

6. CONCLUSION

Banks have implemented e-banking mainly as a response to market demands for this type of services which have become an integral part of their operations. Numerous risks related to electronic banking that both banks and their clients face, have made the implementation of an efficient process of risk management in electronic banking even more important. Furthermore, it is important to point out the fact that it is necessary to constantly adjust the elements of risk management process in accordance with regulatory requirements, technological innovations, growing demands of global financial market and new risks. It is also necessary to pay even more attention to non-financial risks and their management. Examples which this paper discusses include some of the ways of risk management in e-banking which may be related to regulatory or the achieved level of technological development of a particular country. [6]
The implementation of an efficient electronic banking system is a consequence of a growing competitiveness among financial institutions, and their tendency to differentiate themselves by offering safe e-services to their clients. This stems from the fact that further development and survival of a bank precisely depends, among other things, on how efficient and adequate is its process of risk management which would reduce the possibility of negative financial results, which could in turn, jeopardize bank's survival on the financial market.

LITERATURA

[1] ABU-SHANAB, E.; MATALQA, S.: *Security and Fraud Issues of E-banking*, International Journal of Computer Networks and Applications (IJCNA) Volume 2, Issue 4, 2015., Available at: http://www.ijcna.org/Manuscripts/Volume-2/Issue-4/Vol-2-issue-4-M-04.pdf
[2] CHORNOUS, G.; URSULENKO, G.: *Risk management in banks: new approaches to risk assessment and information support*, ISSN 1392-1258. EKONOMIKA 2013 Vol. 92(1), 2013., Available at: http://www.zurnalai.vu.lt/ekonomika/article/download/1131/599
[3] CONTINENTAL NATIONAL BANK.: *Online Banking Fraud Prevention Recommendations and Best Practices*, Available at: https://www.continentalbank.com/media/26312/online-banking-fraud-prevention.pdf
[4] FINANCIAL FRAUD ACTION UK (FFA UK).: *Fraud the facts 2016 - The definitive overview of payment industry fraud*, 2016., Available at: https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf
[5] GUNAJIT, S.; PRANAV K. S.: *Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication*, International Journal of Pure and Applied Sciences and Technology, ISSN 2229 – 6107, Int. J. Pure Appl. Sci. Technol., 1(2) (2010), pp. 67-78., Available at: http://ijopaasat.in/yahoo_site_admin/assets/docs/Gunajit_Paper-6_Review_.18192851.pdf
[6] HÄRLE, P.; HAVAS, A.; KREMER, A.; RONA, D.; SAMANDARI, H.: *The future of bank risk management*, McKinsey & Company, 2016., Available at: http://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20future%20of%20bank%20risk%20management/the-future-of-bank-risk-management-full-report.ashx

[7] HONG KONG MONETARY AUTHORITY.: *Risk Management of E-banking*, Supervisory Policy Manual, TM-E-1, 2015., Available at: http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-E-1.pdf
[8] JEHANGIR, M.; ZAHID, M.; JAN, S.; KHAN, A.: *Benefits and Risks of Electronic Banking in the Context of Customer Satisfaction*, Journal of Applied Environmental and Biological Sciences, J. Appl. Environ. Biol. Sci., 6(3)112-117, 2016., Available at: https://www.textroad.com/pdf/JAEBS/J.%20Appl.%20Environ.%20Biol.%20Sci.,%206(3)112-117,%202016.pdf
[9] JOVIĆ, Z.; ĆORIĆ, G.; PEJOVIĆ, I.: *Challenges of modern electronic banking*, Sinteza 2016, International scientific conference on ICT and E-business related research, 2016., Available at: http://portal.sinteza.singidunum.ac.rs/Media/files/2016/442-447.pdf
[10] KPMG.: *Internet Banking Updates - The New Electronic Banking and Cybersecurity Requirements*, 2015., Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/Internet-Banking-Updates-ebanking-cybersecurity-201509.pdf
[11] OSUNMUYIWA, O.: *Online Banking and the Risks Involved*, Research Journal of Information Technology 5(2): 50-54, 2013 ISSN: 2041-3106; e-ISSN: 2041-3114, Maxwell Scientific Organization, 2013., Available at: http://maxwellsci.com/print/rjit/v5-50-54.pdf
[12] SINGH, T.: *Security and privacy issues in e-banking: An empirical study of customers' perception*, A macro research project report, 2013., Available at: http://www.iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdf
[13] SOLANKI, S. V.: *Risks in e-banking and their management*, International Journal of Marketing, Financial Services & Management Research Vol.1 Issue 9, September 2012, ISSN 2277 3622, Available at: http://indianresearchjournals.com/pdf/IJMFSMR/2012/September/13.pdf
[14] ZAREI, S.: *Risk Management of Internet Banking*, 10th WSEAS International Conference on ARTIFICIAL INTELLIGENCE, KNOWLEDGE ENGINEERING and DATA BASES (AIKED '11), Cambridge, UK, 2011., pp. 134-140., Available at: http://www.wseas.us/e-library/conferences/2011/Cambridge/AIKED/AIKED-22.pdf