RISK MANAGEMENT BANKING STRATEGIES IN THE INFORMATION AGE

Elena Parnardzieva Stanoevska

ABSTRACT

The importance of the issue that is subject of this research stems out of the significance and relevance of the banking system stability, as a primary economic factor that is particularly apparent in times of financial crises. One of the key reasons for the serious difficulties and the severe financial crisis in which the financial institutions find themselves, is the inappropriate risk management in the banking operations. The increasing financial liberalization and the inventiveness in the contemporary world influence the rising offer of new banking products and services that carry intricate risks with them.
The technology increasingly has, and shall continue to have, a key role in the risk management. In order to be able to adapt to the new global standards and regulations, banks would have to focus their attention towards reduction of transaction costs and to have prudent risk management. This means necessity to use the latest information techniques and technologies in the banking operations that will contribute towards offering new products and services, in higher quantity and at competitive prices.

The implementation of the Basel standards also refers to the need for continuous improvement of the methods and strategies for measuring and strengthening of the risk management processes in the banking operations. Namely, in order to respond to the increasingly complex banking system to the need of international harmonization of the banking regulation and the need to strengthen the resilience of the banks towards financial distresses, the Basel Committee on Banking Supervision (BCBS) continuously revise the Basel standards introduced back in 1988. The long-term trends in the banking sector impose the need to use new, stricter methodologies for quantitative and qualitative risk measurement and management, including the need for development of new techniques that will enable their successful implementation. The reoccurrence of the financial crisis only confirms the fact that there is still room for further improvement of the risk management methodologies that were used.

In this paper, special attention is paid to identifying methods and proactive strategic approaches that banks should adopt in order to build a strong team and efficient risk management processes in the information age. The rapid development of e-banking brings about benefits, but also risks. Risks in e-banking should be timely identified, controlled and properly managed by banking institutions. As it shown in this paper the technological complexity of the activities related to e-banking, as well as their rapid development particularly affect the intensification of strategic, operational and reputational risk. Analytic and field research was used for preparation of this paper. Additionally, analysis and synthesis methods have been applied. Internet was used as a major tool to approach data and literature.

KEYWORDS

risk management, banking system, information and communications technology

JEL CLASSIFICATION CODES

G210, G32, O33

1. INTRODUCTION

The continuous process of technological innovations and the globalization of the business operations is increasingly encouraging mutual networking between banks, companies and individuals. The speed, security and level of automatization in the execution of the financial transactions are of crucial importance today. The money is no longer the primary focus in the banking operations, but the focus is shifting towards successful management with the banks' assets and increased client trust. The banks that will not be able to timely apply the new technology due to high initial costs or technical issues risk losing the clients to those that penetrate the market first. In that regard, it is necessary for each bank to make timely and adequate strategic assessment, risk analysis and security review during the introduction of e-banking.

The beginning of e-banking dates back in the early 1970s. Just a decade ago the online banking was seen as a privilege for the younger population. Today, the use of e-banking spreads very fast and has upward trend. According to research carried out by Deutsche Bank (2011), the migration towards electronic, online banking is expected to reach up to 60% of the EU population by 2020. According to a Gallup study (2014/15), nearly six in 10 banking customers (56%) prefer more of a digital than a personal relationship with their bank. In the recent study of the European Commission (2020), Internet use continued to increase with 85% of Europeans surfing the internet at least once per week (up from 75% in 2014). Internet banking as more popular is being used by 66% of internet users in 2019. The continuous process of technological innovations, mainly the competition between the banks, the raise of new players on the market, the wide range of new banking products and services are the main reasons for the mass-scale migration. Today, the widespread of corona virus and economies' lockdown throughout the world additionally contribute to exacerbation of this process. The electronic or online banking combines the information and transaction services. It might not result in creation of new risks but it significantly intensifies and modifies some of the traditional risks. On one hand there are risks related to accuracy of information and their correct distribution and perception; and on the other hand there are risks related to automatization, security and privacy of financial transactions. Hence the need, which is also the objective of this paper, to identify the methods and strategies that are needed in order to strengthen the processes related to risk management in the banking systems in the information age.

The global financial crisis in 2008 that happened primarily as a result of decline of the real estate prices includes, among other reasons, the insufficient attention towards appropriate measurement and management of banking risks. Regardless of the fact that many banks in the United States and Europe operate on the basis of a number of documented policies and procedures, the need to use more modern methods for measuring and managing risks resulted in a situation where the banks faced huge burdens due to bad loans and lack of liquidity in their operations. The long-term trends in the banking sector more and more indicate the need to apply new, more rigorous methodologies for qualitative and quantitative measurement and management of risks, including the need for development of new methods, techniques and strategies that will enable their successful implementation. The reoccurrence of the financial crises only confirms that there is still a room for further improvement of the methodologies currently used for risk management. The banks must be active involved in such improvement.

2. THE INFORMATION COMMUNICATION TECHNOLOGY (ICT) IMPACT ON THE BANKING RISK MANAGEMENT

The globalization of the business operations and the ICT development today encourages increasing networking between companies and individuals who do not know each other. The speed, reliability and the level of automation in the execution of the financial transactions is of crucial importance. In this regard, the money is no longer the main focus in banking, but it is the successful management of their assets and increased trust of the clients. As author Wills pointed out, the trust in the

bank is difficult to gain and result of many years of work, but can be lost very quickly and easily. The banks must be prepared to engage additional forces in order to invoke interest in the clients to request and use other, additional banking services (Wills, 1987). In that regard, the banks that will not apply the e-banking technology in time (due to high initial costs or technical issues) risk to lose clients to those who will enter the market first. Therefore, it is necessary for each bank to start making timely and adequate strategic assessment, risk analysis and review of the security when introducing e-banking application.
The continuous process of technological innovations, the increased competition between banks and the emergence of new players (institutions) in the market create a wide range of new banking products and services. In addition to financial and investment risks, the banks also face many other risks in an e-banking environment. The e-banking, which combines the information and transaction services, may not lead to new risks, but significantly intensifies and modifies some of the traditional risks related to banking operations. On one hand, there are risks related to accuracy of information and their proper distribution and perception; and on the other hand there are risks pertaining to automation, security and privacy of financial transactions. More specifically, the automatic processing of transactions (known as straight-through processing or STP) made possible by e-banking, reduces the possibilities for manual errors (common for manual processing of data) but they also increase the need for organizational, structural and operational adaptability. Seen from a wider perspective, the risks the banks face in e-banking which impact their entire risk portfolio could be classified as follows: transactional or operational risks (especially security and legal risk), credit, market and liquidity risk, regulatory risk, strategic (investment) risk and reputational risk. The practice of many banks who are pioneers in e-banking confirms that effective management of these risks (especially the operational, strategic and reputational risk), with a purpose of further development of e-banking, will enable to use the benefits from the online banking on longer term (UNCTAD, 2007-2008).

Compared to other risks, the strategic risk, as a risk that by nature has a wider range, is one of the most significant risks in e-banking. The strategic decisions that need to be adopted by the senior management bodies in the bank can have the largest implications on all other risks. In a situation of fast technology changes, high competition between banks and raise of new players on the financial markets, a strategy that is badly planned or implemented could expose the bank to significant risk. In order to respond to the demand for e-banking, the banks should primarily develop efficient strategy (which includes cost-benefit analysis, analysis of the available organizational structure, resources, trained staff, etc.) on the use of internet channels and offer of e-products and services to their clients. The banks will be able to respond to the strategic risk only if they have a clear strategy in place, one that will consider all e-banking effects and will be communicated to all relevant business units, with clear business plan and with effective means for control of its implementation.

There are several operational risks that are amplified in an e-banking environment. As a result of use of a complex technology, the following operational risks are intensified:

- The risk of systems and transactions security (including security of data and the identification security). The threats can be caused both from inside and outside the system and they could have serious financial, legal and reputational implications for the banks. There are three common categories of reasons why there could be a disruption in the system security: disrupted security of the system with serious criminal objective, violated security caused by common, accidental hackers and disruptions caused by omissions in the creation of the actual system;
- Risk in maintaining continuous internet (vs. viruses, hackers and similar hazardous events) as a mean required for financial transactions. The full benefits from the e-banking services can be achieved only with 24/7 availability of those services;
- Outsourcing risks. In order to save costs or due to lack of expertise, the banks often use third-party services, especially when it comes to e-banking. The complex agreements between the bank and the outsourced service providers can create significant material risks for the bank because of the potential reduction of its control over those business activities;

- Risk due to lack of sufficient capacity for meeting the needs of the e-banking products. The inappropriate assessment of the potential e-bank product and service users could result in significant financial and reputational damages for the bank because of a system that has been inappropriately configured or tested;
- Legal risk due to inappropriate protection of the client privacy. The banks that will fail to protect the privacy of their clients could easily face regulatory sanctions.
- Risk of money laundering due to reduction of direct face-to-face contacts with the clients. In an e-banking environment, it is almost impossible for the banks to identify whether particular transaction has been carried out by the actual owner and from which location.

The security of information in the new information economy emphasizes even more the importance of trust and building of that trust in the everyday banking activities. The increasing dependency of the banks from information technology and its wide use in the management of financial operations makes the process of risk management caused by inappropriate information systems especially complex. This process includes economic assessment of information systems that bear risks (especially from security aspect) and their comparison against the investments needed for protection. This comes before the need of finding potential solutions. Since the financial institutions usually use similar software programs, there is a danger of systemic risk. Namely, the increasing involvement of many new (non-financial) companies on the financial market can only make the control of links between different stakeholders and the evaluation of risks they are exposed to more difficult (Sokolov, 2007). Hence, when it comes to use of efficient risk management system from perspective of information security (both from aspect of accuracy and security of information and the aspect of security of actual transaction), the involvement of the Government, financial supervisors and regulators is required, who will implement measures for setting minimum standards for information security. They need to help the banks and other financial institutions in the development of methodologies and implementation of risk management policies, in order to ensure security of the financial information.

The reputational risk is also one of the risks that intensify when the banks are using Internet. The reputational risk can especially increase when the system or the e-banking products and services do not work as expected, when there is no relevant and quick communication network, when the system security is compromised, when the clients have problems with products and services they use, when there are errors or abuses by external third parties, etc. The banks can significantly reduce the reputational risk only if they use efficient processes of dealing with unwanted events caused by the Internet, as well as with timely and comprehensive education of the clients on protection from security risks – in other words, ensuring they comply with the safety recommendations.

In order to respond to the challenge related to managing risks stemming out of the features of the e-banking and the new technology, it is necessary to review or expand the existing principles in risk management, which will remain applicable in e-banking environment. In that regard, the BCBS[1], in order to assist the regulators and banks in defining their policies and procedures for risk control in the newly-established environment, identified a total of fourteen e-banking risk management principles. These principles are not absolute requirements – on the contrary, they are just guidelines that can help the banks mitigate the e-banking related risks. There is no unified approach in managing the e-banking risks. The technology solutions and standards pertaining to e-banking should be defined by the national regulatory bodies in accordance with the national needs and technology development in the national economy. The banks will afterwards start developing, adapt and apply processes of e-banking risk management, depending on the regulatory requirements and policies established by the national supervisory authorities, in accordance with the risk profile, operational structure and their corporate management structure.

[1] The Basel Committee for Banking Supervision has been implementing research activities on the impact the e-banking and e-money have on the risk management process since 1998. It established the Electronic Banking Group in 1999 for this purpose. This Group includes bank supervisors and bank representatives from many countries in the world and published a Report in July 2003 on the Risk Management Principles in the Electronic Banking.

The core principles for e-banking risk management proposed by the Basel Committee for Banking Supervision (BCBS, 2003) can be clustered in three categories that mutually overlap:

a) Continuous supervision by senior management bodies and boards

Since the senior management bodies of the bank are responsible for development of the business strategy and for supervision and control of the management that manages the risks, they are expected to adopt clear and documented strategic decisions on whether the bank will offer e-banking services. In that regard, they need to implement measures for continuous updating and correcting of the existing risk management policies and procedures for the purpose of integrating the new risk management processes in the e-banking environment, that is, to cover the current and future e-banking activities planned. Without strategic analysis and analysis of revenues/expenditures, the bank will be exposed to cost underestimation or overestimation of revenue risk, in relation to the decision for introduction of e-banking. It is necessary to do analysis of all risks that could stem out of the proposed e-banking activities and also to identify the relevant processes for their reduction to minimum and continuous monitoring. The highest management bodies in the bank need to be sure that they have the sufficient professional and qualified staff that will be able to respond to the technical character and the complex applications related to e-banking. The increased reputational risk that could be the result of implementation of e-banking requires vigilant monitoring of the operating systems, the needs of the clients and timely reporting to higher bodies in case of incident events.

The Internet is an open and global network available to everyone. The differences that exist between the countries in terms of legislation for issuing permits for work of banks, the requirements for supervision and client protection increase the need to strengthen the control over the banking security, especially in terms of development and maintenance of control of the infrastructure security. Namely, in order to reduce the legal and regulatory risks, it is necessary to introduce comprehensive processes for control of the security and risk management in e-banking environment.

b) Control of security in e-banking environment.

The senior management bodies of the bank are responsible for introduction of processes relevant for e-banking security control. These processes need to include use of relevant procedures for authorization, access control, identity verification measures, limitation of activities of internal or external users, adequate infrastructure for security, reduction of risks from externalization of the banking activities (involvement of partners, outsourcing, etc.), measures for checking authenticity of transaction data, documentation and information. The ensuring of continuous control of the e-banking security aims to reduce the future internal or external threats to the e-banking security. For example, if the bank does not do adequate identification and protection of clients, unauthorized persons can easily obtain access to the e-banking accounts, find confidential information or perpetrate other criminal acts. These frauds could have negative impacts on the reputation of the bank and lead towards greater financial losses. Essentially, the permanent control of the e-banking security should enable full protection of the clients in terms of publishing of information in case of their business use as well as protection of their personal data.

In e-banking environment, the bank should be able to provide documentation on the e-banking transactions. More specifically, in a highly automatic environment, where all transactions are electronic, the banks face the challenge of ensuring effective and independent internal controls, especially for the key e-banking activities and applications. The internal controls can be significantly weakened in one bank if there are no clearly documented traces of all e-banking activities. In that regard, it is necessary to have clearly documented audit notes on all e-banking transactions.

c) Managing legal and reputational risk in e-banking.

In order to reduce the legal and reputational risk to a minimum, the bank that deals with e-banking in the country and abroad must adapt the manner in which it publishes information, the

clients' privacy protection and to adapt the website in accordance with the legal regulatory rules applicable in the country where the bank plans to offer such services. Furthermore, in order to retain its legal and reputational risk as well as the operational risk, the bank must be able to offer e-banking for all end users and those services must be available in all circumstances.

The e-banking use is increasingly emphasizing the importance of banks being ready to meet the high demands of the clients, especially in terms of fast processing of transactions and the 24/7 availability of the electronic service. Adequacy analysis of the bank capacity should be carried out, in terms of capacity in relation to the overall market environment, the e-trade development dynamics, the level of acceptance of the e-banking products and services by the clients, etc. In other words, in order to implement the e-banking, the banks must efficiently plan their capacity (to assess their capability), to prepare plans continuity of the business processes, contingency plans (including the communication strategy) and to clearly define the manners and strategies which they would use in a case of contingencies.

If seen from perspective of the use of modern ICT in banking operations, the latest ICT increases the risk management efficiency, in terms of their timely identification and minimization. For example, with the use of new instruments (collateral for debts, development of derivate markets) and online techniques, the crediting process benefits from better assessment and management of the credit risk. Additionally, the use of new technology which helps to identify more quickly and easily the market risk, especially the risk of change in price of goods, significantly contributes for easier control and reduction of that risk in the banking operation. We can therefore conclude that, by engaging new processes and technologies for protection of the information systems (from unauthorized hijackings, manipulations, modifications or damaging), the banks can significantly contribute towards reduction or even complete elimination of the consequences caused by specific risks on its' operations.

3. METHODS AND STRATEGIES FOR STRENGTHENING THE BANKING SYSTEMS RISK MANAGEMENT IN THE INFORMATION AGE

The risk management process in a situation of increased use of contemporary IT technology in the operations of the commercial banks is becoming increasingly relevant and complex. In addition to the great importance of strengthening of growth and development of the banks, the information technology can also cause side effects on the business banking operations. Namely, it continuously pressures the senior management to more frequently reconsider the strategic approach towards the risks. Although the rapid implementation of modern ICT does not change the traditional banking risks, it significantly increases and modifies them, and also impacts the risk profile of the bank. The application of complex information technologies in the implementation of the banking activities means that the strategic, operational and especially the legal and reputational risk are gaining increasingly prominent place in the risk management process. The electronic banking can create many legal and regulatory uncertainties, that is, it can become more difficult to identify the contracting parties, to determine whether the operator or the users comply with all relevant legal obligations and regulatory regimes, etc.

The biggest threat today for reduction of the ICT functionality and efficiency, are the increasingly frequent attacks on software applications, websites and portals – the security of the new technology. In that regard, the ICT results not only in intensifying of some risks but some of them frequently overlap in the pragmatic banking operations, hence the need for their appropriate classification. For example, the breached security (unauthorized access to client information) can be classified as operational risk, but such an event also exposes the bank to legal and reputational risk. When there is a high correlation of the risks, and when the risks overlap in the business units, it is practically very difficult, almost impossible, to measure and efficiently manage them. In order to resolve these issues and avoid or reduce the business operation risks, the banks, especially the persons at senior management positions, are in charge of

developing clear institutional business strategy as well as risk management strategy – in other words: efficient identification, measurement, control and monitoring of the expected risks. They are responsible for establishing organizational structure that has clearly defined competencies and responsibilities, both of the persons and organizational units who are in charge of risks management and of those responsible for taking risks.

In order to build a strong team and efficient risk management processes, the banks should use the following proactive strategic approaches in the risk management:

a) Rethinking and integration of the risk appetite into the business strategies.

The Supervising and the Management Boards are responsible for defining the acceptable risk level and setting the relevant limits. The frequently occurring financial crises only confirm the need for the supervisory boards to shift their focus from the price of shares and the profitability, towards the risks. The efficient risk management requires to exactly calculate and determine the level of acceptable risk for each specific risk type and for each specific business unit. In that regard, the operational and reputational risk are gaining higher place on the agenda. However, vaguely established business objectives and the inappropriate communication could easily result in a termination of the link between the risk parameters established by the senior management boards and their permanent monitoring in the daily implementation of the business activities. Furthermore, the banks (due to the lack of appropriate technology, analyses, organizational setup or control) are not always able to determine whether particular business decisions are in accordance with the initially defined risk appetite[2]. It is therefore crucially important that every bank, in order to enable effective implementation of the defined risk appetite, ensures the following (BCBS, 2013):

a) effective aggregation and processing of the risk data;

b) reporting on the risk profile, that is, successful transfer of the defined risk level parameters to specific business units and to the level of bank counter.

Ensuring the existence of risk database and their effective aggregation and processing will help the banks to preemptively anticipate of the problems and improve the likelihood of finding alternative solutions towards greater financial stability. Banks still struggle to secure greater transparency of the risk management process beyond their senior management boards, that is, to strengthen the risk management culture at the level of specific business units. In order to overcome this situation, those responsible for risk management should be vested with greater authorizations in order to be able to contribute towards strengthening of the risk management culture in the bank.

b) Strengthening the risk identification processes.

The identification and classification of the potential risks in the business operations are among the most important processes in the risk management. The banks need to have holistic approach towards the risk management and to be cautious in the development of policies and procedures for their identification. The risk identification process can be significantly improved only if continuous daily monitoring of the risks is introduced, as well as establishment of stricter system for risk assessment in the banking portfolio, including introduction of clear procedures for reporting and monitoring of the new clients. In order to identify the many new functional risks (risks that occur often and overlap in many business units), many banks establish special committees that include representatives from a number of organizational units (finances, risks, IT, compliance, etc.). This is the way the banks improve the policies and procedures for approval of new products, with inclusion of a special risks group in charge of development, approval and monitoring of the procedure during its entire lifecycle.

[2] Risk appetite is a level or type of risk which, in accordance with the business objectives set and the obligations towards the shareholders, the bank is able and willing to undertake in the implementation of its business activities. (Anderson and Associates, 2010)

c) Focus on new risk groups.

The information age brings new and intensifies some of the existing risk types in the agenda of the supervisory and management boards of the banks. In view of the intensified risks, the banks need to strengthen their management, especially in the following key risks: credit, operational, liquidity, market, strategic and reputational risk. In that regard, attention needs to be paid on introducing clear policies and procedures, standardization of processes and controls, improvement of data collection processes, strengthening of IT systems security, development of relevant methodologies and matrixes for quantifying of risks, etc. In addition, the implementation of stress test and devising scenarios and analyses for each risk type on regular basis is of significant relevance for forecasting of the value inputs in the processes of strategic planning and capital determination.

In the information economy, efficient risk management is about greater diversification of clients, retention and direction of the most solvent clients and attracting clients towards more productive banking products. According to Ernst and Young (2010) there are three ways that can significantly contribute towards building a comprehensive, integrated strategy for risk management. The successful implementation and continuous improvement of the strategy for risk management can only be achieved with continuous:

a) Improvement of the data reporting and submission processes;
b) Improvement and strengthening of instruments and methods for measuring, assessment and forecasting of risks; and
c) Use of modern technology as a prerequisite for achieving greater efficiency.

The senior managers (members of Supervisory and Management Board) usually receive operational reports of individual business units with data pertaining to past periods. In order to make timely and efficient business decisions in an information age, the real challenge for the banks is to have the possibility to prepare reports, on more frequent basis, that will show true and realistic data, in real time, which will then help review, analyze and synthesize risks that are common for a number of business units.

The banks need to have sophisticated forecasting instruments that will help the senior management more easily forecast and understand the implications of specific market events and risks. In that regard, instead of models based on historical data and assumptions, the banks need to strive towards applying forward looking models (for scenario of planning and stress testing) which assume a low probability of occurrence of a particular event, but with high impact on the business operations. Instruments, such as simulations and visual representation, enable the banks to create, test and compare various strategic decisions. There is, of course, a danger of these forecasting models could become very complex, with too many assumptions and variables that will further complicate their interpretation, especially when used as a tool for making business decisions. Therefore, the banks should judge for themselves whether they will rely on the results of highly sophisticated models when making the key business decisions, or simply use current business intuition (God feelings), or use a combination of both methods.

For the purpose of efficient risk management, the executives of the banks must have clear vision for implementation of new technology, in a sense of support and improvement of the risk management processes. The new technology brings many advantages in terms of fast distribution of new products, in the same time reducing the development and maintenance costs. However, the implementation of new IT in the banking operations requires additional capital and know-how. On the other hand, the economic crises and the increased competition are reducing the capital the banks need to invest in new information technology. In view of the increased costs for implementation, the banks approach the challenges related to the new information technology in proportion with their abilities – size and complexity of the business activities. The larger banks usually can afford larger and deeper investments in systemic information, contrary to the smaller banks which usually implement IT projects for specific systems at particular business unit level. The differences in the level of development of the banks, that is, the different

implementation of the new IT will certainly produce different results and benefits for the banks from their practical implementation.

4. CONCLUSIONS

The Internet penetration today is stronger than ever. According to the EU agenda, 9.2 billion Euros are expected to be invested in the key digital technologies for the period 2021-2027. The goal of the new investment Digital Europe Program is to ensure that all Europeans possess the skills and the necessary infrastructure to meet a full range of digital challenges. However, the e-novelties in the information economy need to be analyzed from both sides of the equation, i.e. positive and new opportunities, on the one hand, and challenges and dangers on the other. In that regard, the fast development and use of the e-banking brings about benefits but also risks. The e-banking risks would have to be timely identified, controlled and properly managed by the banking institutions. The field research implemented by the BCBS confirmed that the e-banking related activities do not contribute to the emergence of new risks, but they simply modify and intensify the traditional risks that could significantly affect the overall risk portfolio of the banks. The technological complexity of the e-banking related activities and their fast development intensify the strategic, operational and reputational risk.

The use of modern ICT in the banking operations increases the risk management efficiency in terms of timely identification and minimization of those risks. The information security requires harmonization of the technical, managerial, regulatory and legal aspects of the operation. In that regard, banks are recently much more concerned for promotion of the information security since they belong to the economic agents that largely apply the ICT innovations in their operations. The threat of cyber theft in information economies increasingly makes pressure to the international community to establish common information security processes and practices.

By engaging the new processes and technologies for protection of the information systems (from unauthorized takeovers, manipulations, modifications or damages), banks can significantly contribute towards reduction or possibly complete elimination of the consequences caused by specific risks on their operations. Therefore, the use of new ICT and utilization of all its advantages requires creation of active business policies and processes for risk management. As shown in the paper, banks need to adopt new methods and proactive strategic approaches in order to build strong teams and efficient risk management processes in the information age. In the future, those banks that do not apply proactive strategic approaches in the risk management and are not able to meet the basic criteria for information security would have to marginalize the risks appetite in their operations.

REFERENCES:

Anderson Richard and Associates (2010) “Risk Appetite-reality v.aspirations”, Independent Governance Risk and Assurance, Working Paper no. 2, pp.1-8

Bresnahan, Timothy F. (2001) “Prospects for an Information Technology-Led Productivity Surge”, NBER, Working Paper, version 5/4/01, pp. 1-24

Brown, Jeffrey (2000) “Does the Internet Make Markets More Competative? Evidence from Life Insurance Industry”, John F. Kennedy School of Government, Harvard University, Research Working Papers Series, pp. 1-27

Basel committee on banking supervision–BCBS (2003) “Risk management principles for electronic banking”, Bank for International Settlements

Basel Committee on banking supervision–BCBS (2005) “Compliance and the compliance function in banks”, Bank for International Settlements

Basel committee on banking supervision – BCBS (December 2010) "Basel III: A global regulatory framework for more resilient banks and banking systems", Bank for international settlements, pp. 1-77

Basel committee on banking supervision – BCBS (2013) 'Principles for effective risk data aggregation and risk reporting", Bank for international settlements, pp. 1-28

Chavan, Jayshree (2013) "Internet Banking-Benefits and Challenges in an Emerging Economy", International Journal of Research in Business Management(IJRBM), Vol.1, Issue 1, June 2013, 19-26

Committee on payment and settlement systems (2004) - Survey of developments in electronic money and internet and mobile payments

Coppel, Jonathan (2000) "E-Commerce: Impacts and Policy Challenges", OECD, Economics Department Working Papers No. 252, pp.2-26

Daniela Yu and Jon Hughes (2016), Struggle for Banks: Migrating Customers to Digital, Business Journal

Deutsche Bank Research (2011) "Update on online and mobile banking", www.dbresearch.com

Dynamics of Innovation in E-Banking, S.Singh, S.S.Chhatwal, Y.C.Heng, T.M.Yahyabhoy, ECIS 2002, June 6-8, Gdansk, Poland

Ernst and Young (2010) "Three ways global banks are strengthening risk governance processes", Annual Global Bank Risk Survey Report

Ernst and Young (2010) "Three ways banks are rethinking risk strategies", Annual Global Bank Risk Survey Report

Elena Parnardzieva Stanoevska (2014) "Influence of the Information Economy on the Management of Banking Risks - International Practices, Conditions and Perspectives in the Republic of Macedonia "- Doctoral dissertation, pp.1-266

European Commission (2020), Digital Economy and Society Index (DESI) 2020 Use of internet services

Jacobodies, Michael G. "Rethinking the impact of information technologies on transaction costs and outsourcing practices", http://blue.temple.edu

Kapital-Banks and Insurance (2007), "Banks grow faster than the economy", pp.4-9

Leonardo Martinez-Diaz (2007) "Banking Sector Opening: Policy Questions and Lessons for Developing Countries", The Brookings Institution, Washington, DC 20036, Policy Brief 2007-01 Global Views

Licht, Gerorg and DietmarMoch (1999), "Innovation and information technology in services", Canadian Journal of Economics, Vol.32, no.2 pp. 303-383

OECD (1999) "A Global Action Plan for Electronic Commerce", Prepared by Business with Recommendations for Governments, 2-41

OECD (2000) "A New Economy? The Changing Role of Innovation of Information Technology in Growth" , www.oecd.org, Chapter 4, pp. 73-80

Sokolov, Dmitri (2007) "E-banking: Risk Management practices of the Estoninan Banks", Published in Working Papers in Economics, School of Economics and Business Administration,Tallinn University of Technology Discussion Paper, pp.21-37

Solbes Pedro (2001) "The internet economy: impact on EU productivity and growth", European government Business Relations Council meeting, Brussels, pp. 1-5

Transforming Consumer Banking Through Internet Technology (2013) http://www.dynamicnet.net/news/white_papers/internetbanking.htm

United Nations Conference on Trade and Development (2007-2008) "E-Banking and E-Payments: Implications for Developing and Transition Economies", Information Economy Report, Geneva, Chapter 5

Wills John (1987) "The management of Banking risk" Whitman and son (Publishers) LTD, London

Wigand, Rolf T. and Robert I. Benjamin "Electronic Commerce: Effects on Electronic Markets", www.ascusc.org/jcmc/vol1/issue3/wigand.htm