

## **ELECTRONIC BANKING RISKS: CHALLENGES, SECURITY CONCERNS, AND MITIGATION STRATEGIES**

**Sara BIXHAKU**

M.sC. , "Eqrem Çabej" University, Gjirokastra, Albania  
[sarabixhaku@gmail.com](mailto:sarabixhaku@gmail.com), ORCID: 0009-0005-6084-2175

**Antoneta POLO**

Assoc.Prof., "Eqrem Çabej" University, Gjirokastra, Albania  
[neta\\_polo@yahoo.com](mailto:neta_polo@yahoo.com), ORCID: 0000-0003-2126-5019

**Ilirjana ZYBERI**

Assoc. Prof., "Eqrem Çabej" University, Gjirokastra, Albania  
[izyberi@yahoo.com](mailto:izyberi@yahoo.com), ORCID 0000-0003-0591-1738

**Enkela CACA**

Assoc. Prof., "Eqrem Çabej" University, Gjirokastra, Albania  
[ebabaramo@yahoo.com](mailto:ebabaramo@yahoo.com), ORCID: 0009-0003-8363-9191

### **Abstract**

Electronic banking has transformed the financial industry by offering convenient, fast, and cost-effective services to consumers and businesses. However, the digitalization of financial transactions also introduces a range of risks and security concerns. Key challenges include phishing attacks, identity theft, malware, and system vulnerabilities, which can lead to financial loss and erosion of customer trust. Additionally, the rapid evolution of technology and increasing regulatory demands pose significant operational hurdles for banks. This paper explores the major risks associated with electronic banking, highlights the most pressing cybersecurity threats, and examines both technical and administrative strategies to mitigate them. Rapid technological development makes the Internet the best way to provide customers with banking services regardless of time and geographic boundaries. Compared to traditional banking, electronic banking provides ease, convenience and access to their customers so that they can use the banking site for all types of transactions in a secure environment. Customers can interact with the banking site 24 hours a day and seven days a week. Despite the many benefits offered by this service, it remains a double-edged sword and is not used by every customer, because the growing distance between the bank and customers can lead to a lack of trust and increased concerns for safety. A particular risk comes with trying to integrate new channels with existing channels. An important step that banks must take before undertaking any kind of transformation is to ensure that online banking risk is properly addressed. Addressing e-banking risk includes a number of measures that banks and users can take to minimize and manage these risks. The purpose of this chapter is to identify the types of risks associated with electronic banking and to propose some of the main methods for dealing with these risks. These include multi-factor authentication, data encryption, customer awareness programs, and robust regulatory compliance. Addressing these challenges requires a holistic approach that combines technology, policy, and stakeholder collaboration. By strengthening digital security infrastructures and fostering a culture of cyber awareness, financial institutions can better protect their systems and customers in an increasingly digital financial ecosystem.

**Keywords:** operational risk, interest rate risk, transaction risk, reputation risk, strategic risk

**JEL Classification:** G21, D14

### **Citation:**

Bixhaku S., Polo A., Zyberi I., Caca E., 2025. "Electronic banking risks: Challenges, security concerns, and mitigation strategies", Sustainable Regional Development Scientific Journal, Vol. II, (1), pp. 44-53

## 1. Introduction

Perceived risk has long been an important factor influencing customers' decision-making when purchasing products or consuming services. This concept becomes particularly important in the context of electronic banking, where the use of technology is often perceived as an uncertain and complicated process. According to various studies, including those by Mitchell [1] and Davidow [2], customers often face ambiguity and uncertainty due to the nature of technology, which brings new and unfamiliar stimuli.

When they decide to use electronic banking, customers are exposed to various risks, such as the availability of services, their performance and security. This perception of risk is supported by empirical research, such as those of Ho and Ng [3] and Lockett and Littler [4], which confirm that the use of electronic banking systems is closely related to the sense of risk.

In this context, operational risk, credit risk, interest rate, liquidity, price, exchange rate and transaction risk are among the main risks that banks and their customers encounter in electronic services. These risks have a significant impact not only on the operation of banks, but also on the customers' perception of their safety and reliability.

The paper explores these aspects of risk in electronic banking, analyzing the main factors that contribute to them and the impact they have on the performance of financial institutions and the customer experience. Furthermore, it examines the importance of effectively managing these risks to ensure that banks provide quality services and maintain their reputation in an increasingly competitive market.

## 2. Literature review

E-banking is defined as "an online portal through which consumers can perform various types of banking services ranging from paying bills to making investments" [5]. With the exception of cash withdrawals, internet banking gives customers access to almost any type of banking transaction at the click of a mouse [6]. Indeed, the use of the Internet as a new alternative channel for the distribution of financial services has become a competitive necessity instead of just a way to achieve competitive advantage with the advent of globalization and fierce competition [7, 8].

Banks use online banking as one of the cheapest channels of providing banking products [5]. Such a service also saves time and money of the bank with an added benefit of minimizing the possibility of bank teller errors [9]. Wise and Ali [10] argued that many banks in their country want to invest in ATMs to reduce the cost of branches since customers prefer to use them instead of using a branch to do business. The financial impact of ATMs is a marginal increase in fee income significantly offset by the cost of a significant increase in the number of customer transactions. The increase translates into improved customer loyalty leading to customer retention and increasing the value of the organization. E-banking is a lower cost delivery channel and a way to increase sales. Karjaluoto et al. [11] argued that "electronic banking is no longer limited by time and geography. Customers worldwide have relatively easy access to their accounts, 24 hours a day and seven days a week". The author further argued that, with online banking, customers who used to think that bank branches take too much time and effort are now able to transact at the click of their fingers. Robinson [12] believes that offering Internet banking services enables banks to establish and expand their relationships with customers. There are many other advantages for banks offered by online banking such as, mass customization for each user, innovation of new products and services, more effective marketing and communication at lower cost [13], development of non-core products such as insurance and stock production as an expansion strategy, improving market image, better and faster response to market evolution [9].

Stewart [14] asserted that despite the advantages of e-banking there is a possibility of its failure and this is mainly attributed to the lack of trust of consumers towards electronic channels. There are several other theories about customer behavior that can explain the rate of adoption and acceptance of e-banking. Interesting is the study of Doll [15], who also claimed that the content of product information in the design and presentation of the web are also important factors that affect customer satisfaction.

Mattila and Mattila [16] also asserted that security has been widely recognized as one of the main barriers to Internet adoption and it depends on the availability of Internet service and a number of other social and psychological factors. In the banking industry, customer-bank-corporate relationships remain a key issue where businesses invest to maintain a higher competitive edge in the market [17]. The relationship between banks and corporate clients is the most important factor in the success of new financial services. In conclusion, several empirical studies have examined the impact of internationalization and corporate e-banking on firm performance [18].

The growing popularity of e-banking has drawn attention to legal and illegal online banking practices. Criminals focus on stealing a user's online banking credentials because the username and password combination is relatively easy to obtain and then relatively easy to use fraudulently to access a bank account in internet and to commit financial fraud. To notify users, many banking sites are now including Security Indicators (Si) on their sites. Hua, Guangying [19] conducted an experiment to investigate how users' perception of online banking is affected by the perceived ease of use of the Internet and the privacy policies provided by the Internet banking website. In this study, he also examined the relative importance of perceived ease of use, privacy, and security. Perceived ease of use is of lesser importance than privacy and security. Security is the most important factor influencing user adoption. A particular risk arises with the attempt to integrate new channels with existing channels [20].

Slowly but steadily, bank customers are moving towards internet banking. An important step that banks must take before undertaking any kind of transformation is to ensure that online banking risk is properly addressed. This is very difficult for both customers and banks to determine the best way to use online banking. Also trust plays a very important role. It is very difficult to analyze trust as a phenomenon and it can be almost impossible to analyze trust in the context of e-commerce because of the complexity and risk of e-commerce. Trust will be the deciding factor for the success or failure of e-banking.

### **3. The risks associated with electronic banking**

Customers perceive greater risks when performing services than when purchasing tangible goods [21]. Zeithaml [22] sees services as riskier than products because services are intangible, non-standardized, and often sold without warranty. Customers can rarely return a service they have already consumed to the service provider moreover some services are so technical or so specialized that customers have neither the knowledge nor the experience to assess whether they are satisfied, even after they have consumed the service [1].

Perceived risk has been considered as an important feature that affects the decision-making process of customers when they buy a product or consume some services [1]. Electronic banking is a channel that uses technology and customers perceive the use of banking electronic as a risky decision because services that apply technology present unknown and ambiguous incentives [2]. Therefore, when customers decide to use electronic banking, they are exposed to uncertainties such as the availability, compliance, and performance of electronic banking channels [23].

Ho&Ng [3] and Lockett&Littler [4] empirically support the fact that the use of the electronic banking system is associated with risk. Davidow, W. H. [2], suggested that customers perceive the existence of risk as present in the use of electronic banking services. Similarly, Sarin, S., Sego, T., and Chanvarasuth, N. [23] identified risk as an important characteristic of electronic banking.

#### **3.1 Operational risk**

Operational risk is the risk of loss resulting from inadequate or failed internal processes, systems and people, or external events and actions. As a result, the bank is unable to offer high quality products and services. Risk is present in every product or

Operational risk is the risk of loss resulting from inadequate or failed internal processes, systems and people, or external events and actions. As a result, the bank is unable to offer high quality products and services. Risk is present in every product or service offered. The level of risk is a consequence of the structure of the institution as well as the surrounding environment. Also, the risk will be determined by the nature and complexity of the products and services offered. Systems, processes and technology on which all these products rely will be the main indicator of the level of risk to which the institution is exposed.

Banks face three types of operational risk:

- ☐ Prediction the volume of transactions
- ☐ Information System Management
- ☐ Transfer, delegation (outsourcing)

##### **3.1.1 Forecasting the volume of transactions**

Forecasting the volume of transactions is difficult, therefore one of the biggest challenges that banks operating through the Internet will face is predicting the number of customers and the volume of transactions they will face. Experience has shown that many of the banks that offer electronic services have made a bad forecast of the volume and of course in such a case the bank may face financial and reputational damages and often compromises in terms of security as often to cope with the excessive demand they implement

inappropriate and previously untested systems. In order to avoid this category of risk as much as possible, banks should:

- ☐ do occasional market research
- ☐ implement database systems that ensure sufficient and flexible capacities to cope with changes in demand
- ☐ undertake promotional campaigns and
- ☐ Ensure sufficient staff and development of a suitable business plan

### **3.1.2 Information System Management**

The second type of operational risk that accompanies e-banking is related to the management of the information system. Banks may face the difficulty of an adequate information management to monitor the electronic services they provide as there may be difficulties in configuring a new system that will provide the generated information. So it is necessary that the information generated is complete and available in understandable formats.

### **3.1.3 Transfer, delegation (outsourcing)**

Recently a significant number of banks delegate some related business functions such as security. This is done for cost reduction purposes, but also due to the fact that the bank lacks sufficient expertise to provide it on its own. Transfer is an important function which can create material risks by potentially reducing the bank's control ability over security. Of course, the delegation of functions is not something new, nor is it uncontrollable, but banks should be more careful about the risks that accompany it.

Operational risk is a consequence of inefficient internal procedures and systems. Also, losses caused due to human errors or technical errors can lead to significant amounts of losses and are included in this category, intentional damage to computer systems (hacking damage), theft of information, etc. The problem with these types of risks lies in the fact that it is quite difficult to assess and quantify them. Since the 1990s, the financial sector has experienced losses exceeding \$100 billion estimated as a result of operational losses. In addition, banks must assess all operational risks across products, activities, processes and systems. Banks identify and assess operational risk in all relevant products, activities, processes and their systems. Banks, in order to effectively identify operational risk, consider both internal factors (such as the entity's structure, nature of activities, the quality of human resources, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that may adversely affect the achievement of the bank's objectives.

Also, banks must ensure that any new product, activity, process or system goes through an operational risk assessment process before being put into operation. They should build a system for continuous monitoring of risk profiles and loss exposures. There should be a continuous reporting of information related to the issue of risk analysis in order to take preventive measures in a timely and appropriate manner. Banks should also have appropriate policies, processes and procedures for controlling and mitigating operational risks identified during the risk analysis process. These procedures should be reviewed on an ongoing basis so that risk assessments are always up-to-date. It is also very important for banks to have contingency plans and business continuity plans (BCP: Business Continuity Plan) in place in order to ensure business continuity capability in the event of a crisis or an event that would affect the serious way in the good functioning of all bank processes.

## **3.2 Risk related to the operational system**

With the invention of the electronic "space", a new phenomenon called Electronic Crime appeared. Computer systems or the Internet can be thought of simply as instruments used to carry out well-known criminal acts such as theft, fraud, etc. The birth of the computer and in particular the Internet created entirely new spaces in the market economy and enabled the rapid movement of information within and outside the borders of the European Union. But the Internet brought with it many other negative phenomena related to the creation of new opportunities and spaces to commit fraud and theft using this new technology. Through special equipment and in-depth knowledge in this field, many people managed to interfere with electronic systems and perform unauthorized transactions for financial gain. This situation led to the issuing of new laws which aimed to regulate all these new phenomena.

In a communication from the European Commission, the term electronic crime refers to three categories.

The first category includes types of traditional crimes such as fraud or theft but always committed through the use of computer systems.

1. Fraud: Knowingly telling or telling false facts or events as if they were true for the purpose of financial gain.

2. Identity Theft: Identity theft means stealing someone else's identity information (such as the personal number on credit cards). As in the case of fraud, identity theft is done to help commit other crimes such as stealing bank accounts, paying for various purchases on the Internet, etc.

The second category includes the publication of illegal content on the Internet

The third category includes new types of crimes that are committed precisely as a result of the development of new technologies such as computers and the Internet. Examples of these crimes are:

Spamming - These are advertisements that appear automatically during normal browsing on the Internet or various e-mails that may come to our e-mail address that have an advertising content.

Hacking - Hackers are individuals who possess special computer skills and who manage to intervene inside systems, computer programs or websites by discovering and exploiting the cracks that may be in their security systems.

Malware - Is a category of harmful programs that include viruses, logic/time bomb/Trojan horse, sniffer programs, denial of service attacks, data manipulation, Web spoofing, and Web site defacements. Generally these are carried out by anonymous individuals who can mask their IP addresses, and use someone else's identity.

Investigating such matters is almost impossible, and requires the most trained computer experts who are usually hackers employed by the state itself.

### 3.3 Credit risk

Credit risk is the case when the client does not pay the obligations to the bank, according to the contract he signed with him. Through the Internet, the bank does not personally contact customers who apply for loans. Therefore, this constitutes a challenge for the bank to verify the "authenticity" of the client.

In general, the credit risk of a financial institution is not increased by the fact that the loan originates from an e-banking channel. However, management must take additional precautions when approving loans electronically, including ensuring management information systems are effectively in place to track portfolio performance originating from e-banking channels. Credit risks may increase in the future if the relationship with customers becomes more distant and transient, and if banks do not pay attention to credit standards due to competitive pressures.

The following aspects of online loan origination and approval tend to make the credit risk management process more challenging. If these aspects are not managed properly, the credit risk can increase significantly.

- Verification of the client's identity for online credit applications and the execution of a binding contract;
- Monitoring and control of the growth, prices and continuous quality of the loan created through e-banking channels;
- Collateral evaluation and collateral refinement over a wide potential geographic area;
- Collection of loan payments from individuals over a potentially wider geographical area; AND
- Monitoring of any increase in volume, and possible concentration outside the lending area.

### 3.4 Interest rate risk

Interest rate risk is the result of interest rate fluctuations. From an economic point of view, a bank focuses on the sensitivity of assets, liabilities and income to changes in interest rates.

Interest rate risk is caused by:

- differences between the moment of interest rate change and the moment of current flows (pricing risk);
- from the change of relations between different interest curves that affect banking activities (basis risk);
- from the change of rate relationships along the spectrum of maturities (yield curve risk);
- from interest rate related options included in banking products (options risk).

The assessment of interest rate risk should take into consideration the impact of complex, illiquid strategies or products as well as the potential impact that changes in interest rates will have on commission income. In these situations where trading is managed separately, this refers to structural positions and non-tradable portfolios.

Electronic banking can attract deposits, loans and other relationships from a larger pool of potential customers than other forms of marketing. A greater access to customers who primarily demand the best rates or terms, forces managers to create appropriate asset/liability management systems, including the ability to quickly adapt to changing market conditions.

### 3.5 Liquidity risk

Liquidity risk is the risk arising from the bank's inability to repay its obligations and the bank's inability to manage unplanned changes in financing resources. Online deposits have the potential to attract customers

who focus exclusively on rates. An institution can control this potential volatility and extended geographic reach through its deposit contracts and open account practices, which may include face-to-face meetings or the exchange of correspondence.

Internet Banking can increase the volatility of deposits for customers who keep their accounts only based on rates or terms. Assets/Liabilities and loan portfolio management system should be suitable for products offered through internet banking. Increased monitoring of liquidity and changes in deposits and loans may be necessary depending on the volume and nature of accounts opened online.

### **3.6 Price risk**

Price risk is the risk of earnings or capital derived from changes in the value of tradable portfolios of financial instruments. This type of risk originates from market making, agreements and taking positions in interest rates, foreign exchange, capital and commodity markets.

Banks may be exposed to price risk if they establish or expand deposit brokerage, loan sales or securitization programs as a result of electronic banking activities. Appropriate management systems are needed to monitor measure and manage price risk if assets are actively traded.

### **3.7 Exchange rate risk**

Foreign exchange risk is the case when a loan is disbursed in a currency other than the local currency. Currency risk can be caused by political, social and economic developments. The consequences can be unfavorable if the currency becomes subject to frequent exchange rate fluctuations. Banks are exposed to currency risk if they accept deposits or give loans in currencies other than the local one. Therefore, banks that use internet banking must install sophisticated systems if they are involved in activities that contain currency risk.

### **3.8 Transaction Risk**

Transaction risk is the risk arising from an error, fraud or the inability to deliver products and services, maintain a competitive position and manage information. Transaction risk is evident in every product and service offered as well as in the internal banking control system.

A high level of transaction risk can also exist in internet banking products, especially in those products/services that are not well planned, implemented and monitored. Banks that offer financial products and services via the Internet must be able to meet consumer expectations. Banks also need to ensure that they have the right product, the capacity to deliver it quickly and on time, and the provision of reliable services to enhance reputational trust.

Attacks or interventions in the network of the banking system are one of the main concerns. Studies have shown that banking systems are more exposed to internal than external attacks. This is because internal users have knowledge of the system and can access it very easily. Therefore, banks must have protective audit systems in order to protect Internet banking from external and internal attacks.

The drafting and implementation of the contingency and/or fallback recovery plan is necessary for a bank, because through this plan the bank ensures that it can offer banking products and services even in unfavorable circumstances.

### **3.9 Reputational risk**

Reputational risk is the case when laws, rules or ethical standards are broken. This risk exposes the bank to the payment of fines, penalties, damages and contract cancellations. This risk lowers the bank's reputation. An institution's decision to offer e-banking services, especially complex transactional services, significantly increases its level of reputational risk. Some of the ways in which e-banking can affect the institution's reputation are:

- Loss of trust as a result of unauthorized activity in customer accounts,
- Disclosure or theft of confidential customer information by unauthorized parties (eg, hackers),
- Failure to provide reliable service due to the frequency or duration of service interruptions from temporary systems failure;
- Consumer complaints regarding difficulties in using e-banking services and the institution's inability to solve problems.

Risk of damage to the bank's reputation may arise, even if customers do not suffer any actual damage. If a hacker successfully accesses a bank's website and makes changes, the bank in question may suffer substantial damage to its reputation even though customer balances are secure and the hacker has not

received any financial benefit. This affects not only the bank in question, but can also undermine confidence in the security of e-banking in general and therefore slow down development in this area.

### 3.10 Strategic risk

Before the bank offers an internet banking product, management must consider whether the product and technology match the banking objectives. Also, the bank should take into account whether the resources are sufficient and able to identify, monitor and control the risk in internet banking.

Technology experts along with marketing and operations experts should contribute to the planning and decision-making process for internet banking. New technologies, and in particular the Internet, can lead to rapid changes in competition. Therefore, the strategic vision should define how a product to be offered on the Internet is designed, implemented and monitored. The freedom and global reach of the Internet opens the threat of increased competition from new members who will no longer need a network of branches to operate effectively in any given market. This competition may have started across national borders. Meanwhile, existing players are faced with the problem of what to do with the branch networks they have built up over the years.

Poor investment planning and decisions for e-banking can increase a financial institution's strategic risk. For this, financial institutions should pay attention to the following problems:

- Suitability of management information systems (SIM) to track the use of e-banking and profitability;
- Costs involved in the creation of e-banking technology;
- Designing, providing, and pricing services appropriate to generate sufficient customer demand;
- Costs and availability of staff to provide technical support for dislevels involving multiple operating systems, web browsers, and communication devices;
- Competition from other e-banking providers; AND
- Technical suitability, operational, harmony, or marketing support for e-banking products and services.

### 3.11 Image risk

If a banking institution decides to offer e-banking service, it must take into account that the degree to which its image is exposed to risk increases due to the complex nature of this service.

Image risk is the actual and anticipated impact on earnings and equity arising from negative public opinion. This affects the institution's ability to create new relationships or services or to continue existing relationships. This risk may expose the institution to litigation, financial losses or a decline in the customer base. Exposure to reputational risk is present throughout the bank and includes the responsibility to exercise due care in dealing with customers as well as to provide accurate and timely services to the community.

The effects that e-banking can have on the image of the bank:

- Loss of credibility in case of unauthorized actions on the client's account
- Violation of customer privacy (electronic piracy)
- The difference between customer expectations and the level of service provided
- Difficulty of using e-banking
- Leakage of confidential customer information to third parties
- Not providing the service due to frequent interruptions.
- Customer complaints regarding the use of services and the inability of the contact point to respond to customer questions and uncertainties.

In order to determine what will be the impact of e-banking on traditional banks, the board must assess the effect on the following areas:

- Strategy
- Level of customer service
- Profits and costs
- Advertising expenses
- Financing cost
- Opportunities and threats

It is noted that none of these risks are completely new and unknown. The sector of the bank that analyzes the risk treats all the risks mentioned above as risks present in the activity of traditional banks. The difference is made when e-banking gives a different weight to all these risks. Some of these risks assessed as not very important in the activity of the traditional bank have a different importance in the e-banking dimension.

Well-designed marketing is a way to educate potential customers and limit image risk. Customers should understand what they can expect from a product or service as well as what specific risks and benefits are incurred while using the system. In this way, marketing concepts should be closely coordinated with open statements. A national bank should not market its electronic banking system based on features or attributes

that the system does not have. The marketing program must present the product accurately and fairly. National banks should carefully consider how links to third parties are presented on their Web sites. Hypertext links are often used to enable customers to connect to a third party. These links may represent an endorsement of third-party products or services in the eyes of customers. It should be made clear to customers when they leave the bank's Web site, so that there is no confusion about the specific service or product provider or about the security and confidentiality standards that apply. Likewise, statements must be made so that customers can distinguish between insured and uninsured products. Parent banks should ensure that their business continuity plans (BCPs) include the e-banking business. Regular testing of the business continuity plan, including press and public communications strategies, will help the bank ensure that it can respond effectively and quickly to adverse customer or media reactions.

### 3.12 Legal risk

Legal risk has become an important issue in e-banking, and one aspect of this is how any loss from a security breach should be distributed between banks and their customers. Customers must be responsible for any security breach or any system problem that is due to negligence on their part, and this must be reflected in the conclusion of contracts for internet banking services. But if the damage occurred due to system breakdown, negligence of bank employees, attack by hackers or other parties; the bank should be responsible to cover the damages.

## 4. Conclusions

The rapid development of information technology after the 70s of the last century and especially its use in society in the framework of the technical-scientific revolution could not leave out the banking sector. Every day it is used more and more by banks to serve customers with speed, convenience, efficiency and at an ever lower cost. E-banking has become an integral part of modern banking due to lower transaction costs, twenty-four hour services, increased control over transactions, higher volume of transactions in less time, facilities remote transactions and a much wider group of banking products and services. But in addition to these possibilities, e-banking operations increase the different levels of risk for banks. Furthermore, clients who rely on e-banking services may have a greater lack of tolerance for a system that is unreliable or that does not provide accurate and current information. Through online services, clients have a greater choice and do not need to be connected to one financial institution or another. Clearly, the longevity of e-banking depends on its security, reliability and accountability.

One of the biggest problems with e-banking seems to be the security and protection of information exchanged between the client and the bank. In fact, banking systems always express concern that the use of electronic banking may expose banks, customers and their transactions to electronic interception and possibly fraud interventions. Therefore, banks need to carry out regular risk assessments, keep customers informed and, possibly, prepare to offer compensation if private information becomes public. For this reason, all risks related to e-banking will be recognized, addressed and managed by banking institutions in a careful manner. These risks can be mitigated by adopting a comprehensive risk management program that includes a sound strategic plan. It is important that the extent of the risk management program in a financial institution should be proportional to the complexity and sophistication of the activities in which it engages. E-banking requires new administrative controls and potentially increases the importance of existing controls. Management should evaluate its administrative controls to maximize the availability and integrity of e-banking systems. Effective incident response mechanisms are important to minimize operational, legal and reputational risks arising from unexpected events, including internal and external attacks that may affect the provision of e-banking systems and services.

New technologies, especially the Internet, can lead to rapid changes in competition. Therefore, the strategic vision should determine the way a product that will be offered on the Internet is designed, implemented and monitored. The freedom and global reach of the Internet opens up the threat of increased competition from new members who will not need a network of branches to operate effectively in any given market. Poor investment planning and decisions for e-banking can increase the strategic risk of a financial institution. For this, financial institutions should pay attention to the problems of continuous investments in IT. Electronic (cyber) crime, which is getting stronger every day, is today a phenomenon that also accompanies electronic banking, therefore, to protect against it, continuous cooperation with the information technology bodies, as well as those specialized for the fight against cybercrime. The information technology systems designed for electronic banking must be audited continuously, giving constant importance to their audit, why not also using hackers to prove its stability against attacks of any kind. Continuous cooperation with the Bank of



Albania, as the highest specialized and independent regulatory entity in the banking system, is a continuous necessity for electronic banking as a whole.

## References

- Aljlfri, H.A., Pons, A. and Collins, D. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. *Information Management & Computer Security*, 11 (3), 130-138.
- Annavarjula, M. and Beldona, S. 2000. Multinational-performance relationship: A review and reconceptualization. *International Journal of Organizational Analysis*, 8 (1), 48-67
- Clow, K. E., Baack, D., and Fofliasso, C. (1998) "Reducing Perceived Risk Through Advertising Service Quality Cues", *Service Marketing Quarterly*, 16(2), pp.151-162.
- DeYoung, J. 2001 "The Internet's place in the banking industry", *Chicago Fed Letter*, No.163, pp.1-4.
- F Beha, D Sina, F Ruxho, 2024. "The effect of institutional quality on tourism in designated European Union Mediterranean states", *Journal of Infrastructure, Policy and Development* 8 (6), 3412
- F Beha, F Ruxho., 2024. "The impact of public debt on the economic growth. Evidence for Kosovo", *Global Business & Finance Review* 29 (3)
- Falvian C., Torres E and Guinaliu M (2004), "Corporate Image Measurement: A Further Problem for the Tangibilization of Internet Banking Services», *International Journal of Bank Marfating*, Vol. 22, No. 5, pp. 366-384.
- FJ Teixeira, SSPV Pescada, F Ruxho, C Palma, F Beha, 2024. "GLAMPING IN LOW-DENSITY TERRITORIES: THE CASE OF SANTO ALEIXO DA REASTAURA?? O, *Regional Science Inquiry* 16 (1), 71-80
- Gan, C and Clemes, M. (2006). A logit analysis of electronic banking in New Zealand. *International Journal of Bank Marketing*, 24 (6), 360-383.
- Ho, S. S. M., and Ng, V. T. F. (1994) "Customers' Risk Perceptions of Electronic Payment System.", *The International Journal of Bank*, 12(8), pp.26-39.
- Hua, Guangying 2009. An Experimental Investigation of Online Banking Adoption in China, *Journal of Internet Banking and Commerce*, April, Vol. 14.
- Jayawardhena, C., & Foley, P. (2000). Changes in the banking sector – the case of Internet banking in the UK. *Internet Research: Electronic Networking Applications and Policy*, 10, (1), 19-30.
- Kandampully, J. and Duddy, R. 1999. Competitive advantage through anticipation, innovation and relationships. *Management Decision*, 37 (1), 51-56.
- Karjaluto, H., Mattila, M., & Pento, T. 2002. Factors underlying attitude formation towards online Internet banking in Finland. *International Journal of Bank Marketing*, 20(6), 261-272.
- Krupavicius, A., Šarkute, L., Krasniqi, A., Ladas, Christos Ap. 2024. "Perceived and desired images of society: how (un)equal is society?" *Regional Science Inquiry*, 16(1), pp. 55-70
- Ladas C.A., Ruxho F., Teixeira F., Pescada S., 2023, "The regional economic indicators and economic development of Kosovo", *Regional Science Inquiry*, Vol. XV, (1), pp. 73-83
- Ladas, C.A., and Ruxho F., 2024. "Utilizing Regional Economic Indicators to Identify and Mitigate Economic Disparities in Kosovo." *Regional Science Inquiry* 13 (1): 45–57
- Lampreia M., Teixeira F., Pescada S. P. V., 2024. "The predictive power of technical analysis: evidence from the gbp/usd exchange rate", *Sustainable Regional Development Scientific Journal*, Vol. I, (3), pp. 67-75
- Lincaru C., Tudose G., Cosnita D., Pirciog S., Grigorescu A., Ciuca V., 2024. "Clusters as engines of sustainable employment growth in Romania", *Sustainable Regional Development Scientific Journal*, Vol. I, (3), pp. 10-27
- Lockett, A., and Littler, D. (1997) "The Adoption of Direct Banking Services", *Journal of Marketing Management*, No. 13, pp. 791-811.
- Mattila, A. and Mattila, M. 2005. "How perceived security appears in the commercialisation of internet banking" *Int. J. Financial Services Management*, Vol. No 1, pp 23-34.
- Mitchell, V. W. (1998) "A Role of Consumer Risk Perceptions in Grocery Retailing", *British Food Journal*, 100(4), pp. 171.
- Papajorgji P., Tordi A., 2024. "Using quantitative tools to understand political issues", *Sustainable Regional Development Scientific Journal*, Vol. I, (3), pp. 28-35
- Polo A., Caca E., Zyberi I., Ladas C.A, Ruxho F., 2025. "Foreign direct investment in real estate in Albania and its impact on GDP", *Regional Science Inquiry*, Vol. XVII, (1), 2025, pp. 135-142
- Ruxho F., 2024. "Kosovo employee's perception of economic growth and decent work according to sustainability", *Sustainable Regional Development Scientific Journal*, Vol. I, (3), pp. 53-66
- Ruxho F., Ladas C.A, 2022 "Increasing funding for the regional industry of Kosovo and impact on economic growth" *Regional Science Inquiry Journal*, Vol. XIV. (1), pp. 117-126
- Ruxho F., Ladas C.A, 2022. "Increasing funding for the regional industry of Kosovo and impact on economic growth" *Regional Science Inquiry Journal*, Vol. XIV. (1), pp. 117-126
- Ruxho F., Ladas C.A, Tafarshiku A., Abazi E., 2023. "Regional employee's perceptions on decent work and

- economic growth: labour market of Albania and Kosovo”, *Regional Science Inquiry*, Vol. XV, (2), pp.13-23.
- Ruxho F., Ladas C.A., 2022. “The logistic drivers as a powerful performance indicator in the development of regional companies of Kosovo” *Regional Science Inquiry Journal*, Vol. XIV. (2), pp. 95-106
- Ruxho F., Petropoulos D., Negro D.A. 2024. “Public debt as a determinant of the economic growth in Kosovo”, *Sustainable Regional Development Scientific Journal*, Vol. I, (1), pp. 55-67
- Ruxho, F., Ladas, C. A, Tafarshiku, A., & Abazi, E., 2023. Regional employee’s perceptions on decent work and economic growth: labour market of Albania and Kosovo. *Regional Science Inquiry*, 15(2), pp.13-23
- Sarin, S., Sego, T., and Chanvarasuth, N. (2003) “Strategic Use of Bundling for Reducing Consumers’ Perceived Risk Associated with the Purchase of High-Tech Products”, *Journal of Marketing Theory and Practice*, 11(3), pp. 71-83.
- Sepetis A., Krupavičius A., Ladas Ap. C. 2024 “Social protection in Greece and sustainable development leaving no one behind”, *Sustainable Regional Development Scientific Journal*, Vol. I, (1), pp. 83-92
- Sequeira T., Rego C., Dionisio A., 2024. “Investment and productivity in the agro-industrial sector: a case study”, *Sustainable Regional Development Scientific Journal*, Vol. I, (2): Special Issue, pp. 13-26
- Stavara M., Tsiotas D., 2024. “A combined graph theoretic and transport planning framework for the economic 10 Sustainable Regional Development Scientific Journal, Vol. I, (2): Special Issue, Oct. 2024 and functional analysis of large-scale road networks”, *Sustainable Regional Development Scientific Journal*, Vol. I, (2): Special Issue, pp. 27-40
- Teixeira F., Pescada, S.S.P.V., Ladas C.A., Hulaj M., Ruxho F., Machado V., 2025. “Stablecoin dp2p: innovation and sustainability in fiat currencies”, *Regional Science Inquiry*, Vol. XVII, (1), pp. 95-106
- Tsiotas D., Giannakis E., Papadas C., 2025. “A modularity decomposition model of evolving input-output sectorial structure, *Regional Science Inquiry*, Vol. XVII, (1), pp. 107-133
- Tsiotas, D., Krabokoukis, T., & Polyzos, S. 2020. “Detecting interregional patterns in tourism seasonality of Greece: A principal components analysis approach”, *Regional Science Inquiry*, 12(2), 91-112.
- Tsiotas, D., Polyzos, S., 2024. “Transportation networks and regional development: the conceptual and empirical framework in Greece”, *Sustainable Regional Development Scientific Journal*, Vol. I, (1), pp. 15-39