LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 24, NO. 2(2026)

# PRINCIPLES OF MANAGING AND SUPERVISING E-BANKING RISKS

**Belaiche Meyada [1], Laouar Staihi ilhem[2]**

[1]University Of August 20, 1955 Skikda, Algeria
[2]University Of August 20, 1955 Skikda, Algeria
[1,2] Academic Rank: Grade A
m.belaiche@univ-skikda.dz
i.laouarstaihi@univ-skikda.dz

Received: 01/01/2026 ; Accepted:10/03/2026 ; Published: 15/03/2026

**Abstract**
This study aims to highlight the importance of e-banking risk management principles in enhancing the security and efficiency of digital banking operations amid the rapid digital transformation witnessed by the financial and banking sector. The study addressed the various risks associated with e-banking, including technical risks, cyber threats, electronic fraud, as well as legal and regulatory risks that may affect the stability of financial institutions and customers' trust in digital services. The study also sought to analyze the most important internationally recognized principles and standards adopted in e-banking risk management, with a focus on the role of banking governance, internal control systems, and cyber security mechanisms in mitigating risks and enhancing the protection of data and electronic transactions.
The study adopted a descriptive-analytical approach through reviewing theoretical literature and analyzing the regulatory and technical frameworks related to the subject. The findings revealed that the effectiveness of e-banking risk management represents a fundamental factor in achieving financial stability and ensuring the sustainability of digital banking services. Moreover, the success of banking institutions in confronting cyber threats is closely linked to their ability to develop digital protection systems, adopt proactive risk management strategies, and enhance digital awareness among employees and customers. The study also confirmed that digital transformation in the banking sector requires an integrated regulatory and technological environment that balances financial innovation with banking security.

**Keywords:** E-Banking, Risk Management, E-Banking Risks, Cyber security, Digital Transformation, Banking Governance, Electronic Transactions, Financial Institutions, Banking Security, Internal Control.

## Introduction

In recent decades, the banking sector has undergone profound transformations driven by the rapid development of information and communication technologies, whereby e-banking has emerged as one of the most prominent manifestations of digital transformation within financial and banking institutions. The widespread use of the Internet, the continuous advancement of smart applications, and the growing reliance on digital banking services have reshaped the relationship between banks and customers by providing banking services characterized by speed, flexibility, and efficiency. This transformation has enhanced the competitiveness of financial institutions and enabled them to keep pace with the requirements of the global digital economy. In this context, e-banking has become a fundamental pillar for achieving financial inclusion and improving banking performance, particularly in countries seeking to modernize their financial systems and enhance the quality of their services. Despite the numerous advantages and opportunities offered by e-banking, it has also generated increasing challenges related to electronic risks and cyber threats, which may directly affect the security of banking information, data confidentiality, and the stability of financial systems. The expansion of electronic transactions has increased the likelihood of exposure to cyber attacks, electronic fraud, data theft, technical failures, as well as legal and regulatory risks associated with the use of digital platforms in banking operations. Consequently, e-banking risk management has become a critical issue attracting growing attention from researchers, regulatory authorities, and banking institutions alike. Accordingly, there has been an urgent need to adopt effective

principles for managing e-banking risks, based on scientific, organizational, and technological foundations that ensure a balance between benefiting from digital innovation and mitigating potential risks. These principles include the development of banking governance systems, the strengthening of cyber security mechanisms, the implementation of internal control standards, periodic risk assessment procedures, and the promotion of digital awareness among employees and customers. Such measures contribute to enhancing trust in the electronic banking environment and achieving financial stability. In light of these considerations, the importance of studying the principles of e-banking risk management lies in their role as a fundamental approach to ensuring the sustainability of digital banking services and protecting financial institutions from escalating electronic threats. The significance of this study also stems from its attempt to analyze the theoretical and regulatory frameworks related to electronic risk management and to highlight the role of preventive policies and procedures in enhancing the security and efficiency of electronic banking operations.

Within this context, the study seeks to address the following main research question:
**How can the principles of e-banking risk management contribute to enhancing the efficiency and security of digital banking operations and achieving financial stability amid rapid digital transformation?**
To answer this main question, the study addresses the following sub-questions:
- What is the conceptual nature of e-banking risks and their main sources?
- What are the most important internationally recognized principles and standards for e-banking risk management?
- What is the role of banking governance and cyber security in mitigating electronic risks?
- How can the effectiveness of electronic risk management enhance customer trust in digital banking services?
- What are the major challenges facing banks in implementing e-banking risk management systems?

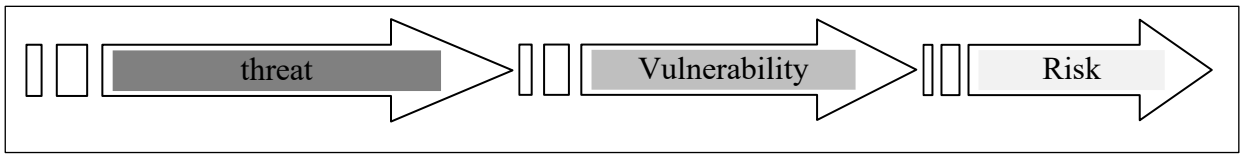
To answer the aforementioned research problem, the topic has been divided into the following sections:
Section One: Concept of Risks
Subsection Two: Types of Banking Risks.
Section Three: Principles of Managing and Supervising E-Banking Risks.
Section Two: Principles of E-Banking Risk Management.
Subsection one: Principles of E-Banking Risk Management
Subsection two: Supervision of Electronic Banking Risks
Section Four: Legal Models for Managing Electronic Banking Risks
Subsection One: The Basel Committee Model
Subsection Two: The European Union Model
Section Five: The Current Legislative and Legal Principles of Electronic Banking in Some Countries
Subsection One: Fundamentals of Legal Regulations for Electronic Banking Worldwide
Subsection Two: Key Legislative Trends and Legal Framework for Electronic Banking in Europe
Subsection Three: Key Legislative Trends and Legal Framework for Electronic Banking
Subsection Four: Key Legislative and Legal Trends in Electronic Banking in China
Subsection Five: Key Legislative and Legal Trends in Electronic Banking in the Gulf Countries

**Section One: Concept of Risks**

The issue of risks is an essential concern for any institution. Risks represent all events that may partially or completely prevent an organization from achieving its objectives or maximizing its performance. They do so by undermining the sustainable benefits of any activity, through: invoking a state of uncertainty, reducing the likelihood of success, lowering opportunities, and increasing threats arising from those activities across three dimensions: profitability, continuity, and growth.

Risks may also increase the likelihood of damage to physical resources or intangible assets due to unforeseen factors over short or long time horizons required to complete the targeted banking activity. The effect of these risks can be assessed objectively by an economic agent using defined numerical probabilities, whereas in cases of uncertainty, the agent cannot assign any potential values in evaluating the situation. This also relates to the institution's security policy. Therefore, risks are defined as attempts to exploit threats, particularly those related to financial position, operational efficiency, and competitive standing.[1]

**Figure 01: Context of Risk Emergence**




**A.Threat (Menace):** A threat is any attempt to disrupt the smooth operation of an institution or to undermine its continuity and chances of success, such as the emergence of new competitors or a lack of competencies and expertise. Threats have three main components:

**1. Target:** The objective the attacker seeks, for example:

- **Privacy:** Exposing confidential information to unauthorized parties.
- **Integrity:** Damaging the efficiency and/or effectiveness of systems.
- **Stability:** Destabilizing positions or situations, or masking an attack on another center by altering event logs.

**2. Method:** The approach used to reach the target. This can be:

- **Direct:** For instance, having a direct access point to the system.
- **Indirect:** For instance, through an intermediary.

The suitable method is determined after collecting sufficient information about the target and understanding the attacker's motives.

**3. Event:** The incident that results in losses, such as fraud, embezzlement, theft, destruction of assets, professional negligence, card forgery, hacking, or eavesdropping on messages.[2]

**B. Vulnerability (Weakness):**

These are points of weakness within the organization through which an attacker can destroy, sabotage, or obstruct the targeted objective. In banking, vulnerabilities can be categorized into five main areas:[3]

[1]Amine Tarazi, **Banking Risk**, Financial Deregulation, and Prudential Regulations, PUF, Paris, 1996, P.10.

[2]Khaled Mamdouh Ibrahim, previous reference, p. 450.

[3]Banque de France, **CreditRisk Management and Financial Stability**, Revue de la stabilité financière, Paris, No. 05, November 2004, p. 116.

1. **Macroeconomic Vulnerability:** Related to the economy in which the bank, its debtors, or the market operates. It reflects the degree of exposure to economic shocks or imbalances. Examples include:
- Rising commodity prices
- Unemployment rates
- Economic growth rates
- Inflation

2. **Credit-Money Vulnerability:** Results from monetary expansion caused by rapid or excessive lending, leading to economic agents being over-indebted.

**3. Risk Estimation Trap:** This occurs when market participants underestimate the actual value of a risk. For example, in lending, this can happen when the credit risk is assessed based solely on the loan's spread, leading to an undervaluation.

**4. Concentration:** This refers to the potential clustering of risks within a limited number of institutions or around specific sectors related to the bank, such as the insurance sector.

**5. Increasing Interconnectedness:** This reflects the rising forms of exchange, integration, overlap, and inter linkages among different units of the financial sector, as well as between economic sectors and global economies.

**Subsection Two: Types of Banking Risks**

Banking activities are exposed to multiple risks around the clock, due to factors related to the customer, the bank itself, or the type of services the bank provides. In this study, we focus on the most significant operational banking risks, both traditional and electronic, as understanding new risks requires reference to traditional ones.

**Branch one: Traditional Banking Operational Risks**

These include credit risk, exchange rate risk, pricing risk, liquidity risk, operational risk, legal risk, compliance risk, and strategic risk.

**1. Credit Risk:** The increasing trend toward globalization in recent years has led to a rise in financial crises and their contagion effects, whereby some countries are affected by crises originating elsewhere. Economic studies indicate that bank crises have been a common factor in most financial crises, whether in developing or developed countries. Credit risks, alongside poor management, have been among the primary causes of bank failures and financial crises.[4] Credit expansion is one of the main banking activities and is associated with several risks, such as the inability or unwillingness of a client or counterparty to fulfill their obligations in relation to borrowing, trade, loss protection, repayment, or other financial operations. Other associated risks include credit concentration and the bank's failure to assess asset quality adequately, which may result in insufficient provisions, exposing depositors' funds to unforeseen losses.[5]

**2. Foreign Exchange Risk (FX Risk):** Banks face the risk of losing part of their assets due to fluctuations in exchange rates. This occurs despite established accounting standards that aim to provide transparency and model-based identification of such risks. For example, maintaining open currency positions during periods of exchange rate volatility increases the

[4]Medhat Sadiq, Banking Tools and Techniques, Gharib Publishing and Distribution, Cairo, 2001,, p. 67.
[5]Brish Abdelkader, Banking Risk Management According to Basel II and III Regulations and the Requirements for Achieving Financial and Global Stability after the Global Financial Crisis, Journal of Humanities, Issue 29, Mohamed Khider University, Biskra, 2013, p.27.

market risk the bank is exposed to. Open positions include both spot transactions and various forms of derivatives**.**

**3. Interest Rate Risk:** This risk arises from fluctuations in market interest rates, which may result in tangible losses for the bank if there is a mismatch between the interest rates on liabilities and assets.

**4. Price Risk:** Price risk stems from changes in the value of assets, particularly the financial investment portfolio. Both external and internal factors can influence price risk, including local economic conditions and the prevailing business climate.[6]

**5. Liquidity Risk:** Liquidity risk emerges when a bank cannot meet its obligations on time or finance an increase in assets. This negatively impacts bank profitability, especially if assets cannot be liquidated immediately at an acceptable cost.

**6. Operational Risk:** Operational risk mainly results from deficiencies in internal controls or weak oversight by the board of directors. It can lead to financial losses due to errors, fraud, delays in decision execution, inadequate banking practices, or failures stemming from information technology systems.[7]

**7. Legal Risk:** Legal risk may cause a bank to lose part of its assets or increase its liabilities due to insufficient legal opinions, inadequate documentation, engaging in new types of transactions without a governing law, or when new legislation affects the creditor's ability to fully recover their rights on time.[8]

**8. Compliance Risk:** This refers to the exposure of the bank to sanctions, whether in the form of financial penalties or being prohibited from engaging in certain activities due to violations.

**9. Strategic Risk:** This arises from the absence of an appropriate strategy that the bank can follow to achieve its short- and long-term objectives, taking into account general environmental conditions, competitors' actions, and an analysis of the bank's internal strengths.[9]

**Branch Two: Risks of Electronic Banking Operations**

The significant growth in electronic banking operations has created new challenges for banks and regulatory authorities, particularly due to the lack of sufficient experience among bank management and staff to keep up with rapid developments in communication technologies. Additionally, the potential for fraud and scams has increased on open networks such as the Internet, due to the absence of traditional practices that verified the identity and legitimacy of clients.

[6]Medhat Sadek, previous reference, p.68.
[7]Bakhtiar Saber Bayez Hussein, The Bank's Responsibility in Documentary Credit and the Risks it Faces, Dar Shatat for Publishing and Software, Egypt, 2010, p.317.
[8]Tarek Mohamed Khalil Al-Araj, Factors Affecting the Choice of Types of Services and Channels Offered by Electronic Banks – An Analytical Study of the Opinions of a Sample of Customers of Qatari Banks, Doctoral Dissertation, p.61.
[9]Amine Tarazi, Banking Risk, Financial Deregulation, and Prudential Regulations, PUF, Paris, 1996, p.13.

Therefore, the Basel Committee on Banking Supervision emphasized the importance of banks establishing policies and procedures that enable the management of electronic banking risks through assessment, monitoring, and control. According to a report by the Electronic Banking Group (EBG) under the Basel Committee in October 2000, the main risks associated with electronic banking were identified as: strategic risks, operational risks, credit risks, market risks, and liquidity risks**.** These risks have influenced the overall perception of electronic banking operations. The Basel Committee also issued principles for managing these risks in March 1998 and May 2001.[10]

1. **Money Laundering Risks:** The European Committee on Money Laundering defined this process and identified its components. In its 1990 guide, it defined money laundering as "the process of converting funds obtained from criminal activities in order to avoid legal responsibility for retaining the proceeds of the crime."
If anti-money laundering (AML) measures evolve, the methods of carrying out money laundering operations also develop, driven by remarkable technological progress, especially in cross-border operations and electronically executed banking transactions. This includes opening bank accounts via the Internet, transfers, and all other electronic banking operations that can be executed directly.
Given the characteristics of these operations, it is possible to determine the local time of the bank's country and the value of the executed transaction and trace it when the user accesses the system. However, it is difficult to identify the true identity of the account holder, as it is almost impossible to determine the identity of the person executing the operation and the beneficiary, or to ascertain the actual location. This implies that a single individual could manage multiple accounts simultaneously without necessarily attracting the attention of the institutions managing these accounts, since these operations do not require the physical presence of the customer—unless the bank has previously imposed such a requirement under the "Know Your Customer" (KYC) principle. Enforcing KYC can help mitigate risks arising from the lack of customer identification.
Although countries can set requirements for transactions within their borders, the prevailing trend today is that they cannot prevent their citizens from opening bank accounts via the Internet in foreign institutions offering banking services. This also raises issues related to bank cards and money laundering due to the multiplicity of applicable systems. Therefore, there is a need to reconsider AML methods, measures, and procedures, as well as banking security systems and overall financial safety, in light of tremendous technological and electronic developments, which in some cases may provide a rapid and effective tool for carrying out money laundering operations.

**2. Legal Risks:** These are risks arising from the unclear definition of legal rights and obligations resulting from electronic banking operations,[11] especially since many instruments of these operations are still under development, such as electronic records, electronic signatures, contracts, rules for sending and receiving electronic records, recognition of authorities and electronic certification rules, and the enforcement of confidentiality and disclosure. Legal risks also include violations of laws, rules, or regulations, particularly those related to money laundering prevention.

[10] Ali Badran, Modern Management of Banking Risks under Basel II, Al-Muhasib Al-Jaz [The Accountant], Chapter Three, Issue 23, Basel, 2005, p.12.
[11] Ahmed Safar, Electronic Payment Systems, op. cit., p.27.

The main legal challenges include: the acceptance of electronic contracts, their evidentiary value, information security, payment methods, tax challenges, identity verification, electronic signatures, cashless payment systems, digital or electronic money, confidentiality of information, protection against high-tech crime, customer privacy, liability for errors and risks, evidentiary value of electronic communications, electronic banking contracts, intellectual property issues of bank software or databases used by or linked to the bank's website, and contractual relationships of the bank with technology providers, service providers, partner websites, and projects involving mergers, partnerships, or IT collaborations.[12]

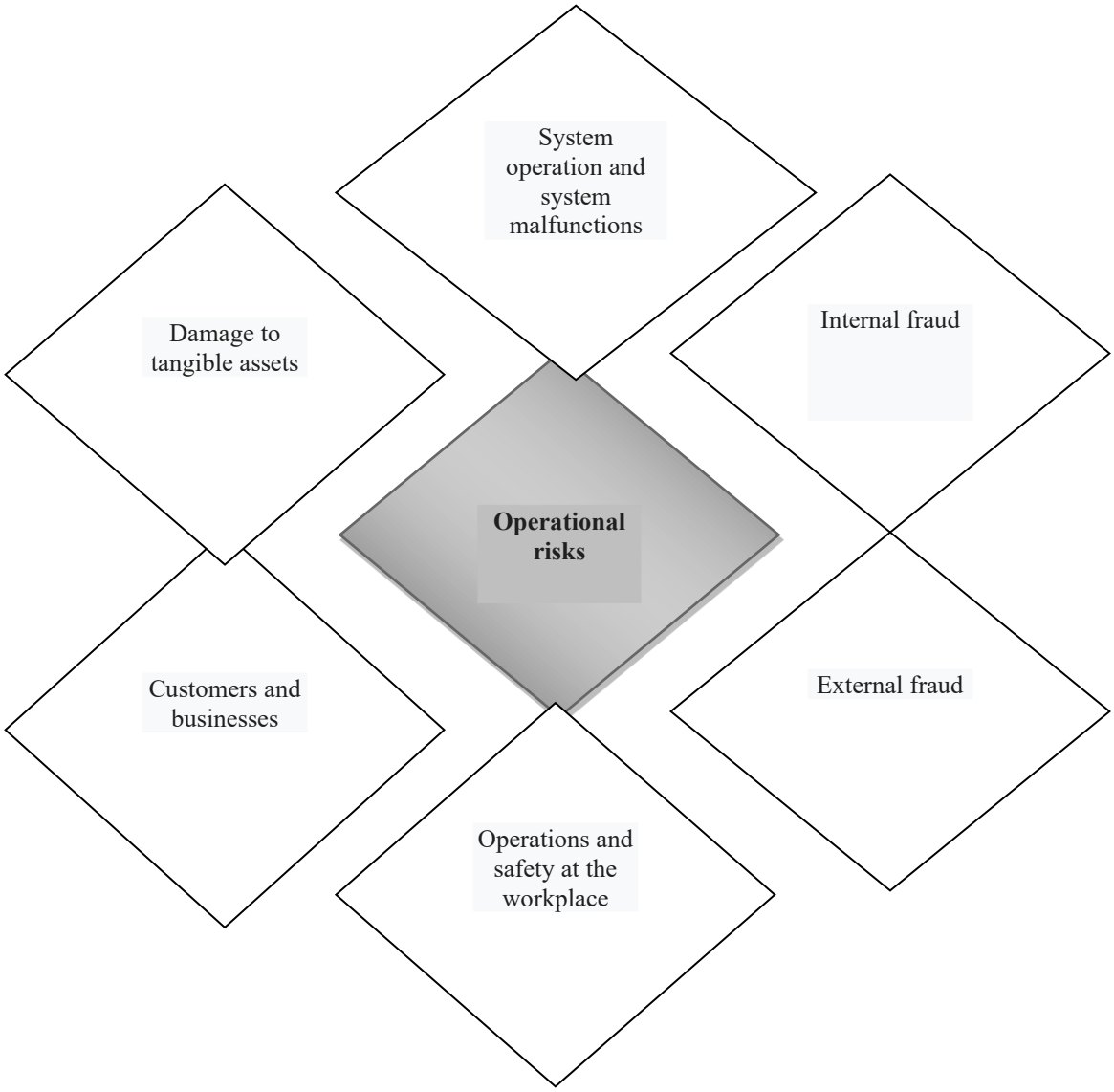
**3. Strategic Risks:** Electronic banking relies on the Internet to provide information to clients as well as to execute requested transactions. Undoubtedly, rapid technological developments and increasing competition both among banks and with non-banking institutions may expose banks to significant risks if the planning and execution of their electronic banking strategies are flawed.[13]
Therefore, banks need to carefully assess how their Internet strategy contributes to maintaining the institution's competitiveness and profitability, while ensuring that it does not inadvertently increase their risk profile. Regulatory authorities should expect banks to evaluate both the benefits and the precautions associated with their strategic choices.

**4. Operational Risks:** Since all banking activities rely on technology, operational risks are among the most challenging risks banks face.[14]
These risks arise from multiple sources. First, many banks depend on third-party providers to manage the technological infrastructure supporting electronic banking operations, meaning that their systems are integrated with those of the third party. Consequently, banks may encounter errors in transaction execution if their electronic banking systems are not properly integrated.
Banks must ensure that these aspects are properly monitored and controlled, and regulatory authorities must assess the bank management's ongoing capacity to achieve this.[15]
Another source of operational risk concerns security: open electronic distribution channels raise challenges for banks in maintaining information confidentiality and integrity, as well as verifying client identities and
Their legitimacy concerning bank accounts, and controlling lawful access for clients to their accounts, becomes especially critical given the rise in fraud, deception, scams, and unauthorized intrusions into the global Internet and legitimate client accounts.
Banks are therefore required to develop appropriate security systems and manage their internal processes in accordance with internationally recognized standards and regulations, particularly regarding client identity verification, the legitimacy of electronic signatures, encryption, and related safeguards. At the international level, global authorities should encourage the development of a comprehensive approach to managing risks related to both internal and external security exposures.
The third source of operational risk is related to information integration, which is a key component of system protection. Banks must improve the coordination of processes within the institution and across its operations to manage relationships effectively with clients, other

[12]ChoulChahra& Madoukh Magda, Electronic Banking: Its Nature, Risks, and Protection, paper presented at Banking System in the Third Millennium: Competition, Risks, Technologies, University of Jijel, Algeria, June 6–7, 2005, p.15.
[13] Ahmed Saqr, previous reference, p. 226.
[14]Mounir Al-Janbehi&Mamdouh Al-Janbehi, previous reference, p. 123.
[15] Ahmed Safar, Electronic Payment Systems, previous reference, p. 26.

banks, and external service providers. Until specific standards for electronic information management are established, banks will continue to face the challenge of implementing effective control measures to ensure the accuracy and integrity of obtained and transmitted information. Regulatory authorities should also encourage banks to continuously monitor the integrity of the information used in their risk management systems.
Additionally, other sources of operational risk include the bank's inability to monitor the availability of the Internet itself. This requires that, as part of emergency planning, banks have alternative means for service delivery in case of disruptions to the Internet network.[16]

**Figure (02): Components of Operational Risks in Banks According to the Basel Committee**




**Source:** Abdelrazak Khalil &HamzaTabi, Managing Electronic Banking Risks According to Basel Committee Standards, research paper published online: www.docstoc.com/, 2004, p.5.

[16]ShoulChahra&MadoukhMajda**,** Electronic Banking: Its Nature, Risks, and Protection, previously cited, p.12.

**5. Reputational Risks:** Reputational risks arise when there is a negative public perception toward the bank, which may also extend to affect other banks, as a result of the bank's inability to manage its systems efficiently or due to a significant security breach.[17]
Reputational risks are related to external developments that may affect a bank's ability to provide its services and products through electronic banking channels.
This underscores the importance for a bank to have a reliable network to support its activities in the field of electronic banking. The bank's reputation can suffer significant damage if it fails to provide online banking services that meet standards of security, confidentiality, accuracy, timeliness, continuity, and rapid responsiveness to the needs and demands of its clients.

**6. Other Risks:** The channels for distributing electronic banking services can impact other traditional banking risks, such as credit, liquidity, interest rate, and market risks. These channels can not only amplify or mitigate the bank's risk profile but may also transform these risks in complex ways in some cases.[18]
Regarding credit risks, distributing banking services through electronic channels may prevent the bank from fully understanding local or international market mechanisms and risks. Consequently, the bank may lack full knowledge of a client's creditworthiness and the adequacy of available guarantees, which are essential for sound credit decision-making.
Regarding liquidity risks, any negative or inaccurate information about the bank can quickly spread via the internet, prompting clients to withdraw their deposits rapidly and potentially causing a liquidity crisis. Conversely, internet banks can increase deposit flows as long as new depositors maintain their accounts under specific conditions and interest rates. Therefore, it is crucial for a bank to continuously monitor changes in its deposits and loans in a precise[19] and ongoing manner.
Finally, concerning foreign exchange risks, a bank may face these risks when accepting deposits from foreign clients or maintaining accounts denominated in foreign currencies. These risks can escalate in situations of adverse economic, political, or social developments in other countries.
Regulatory authorities must ensure that a bank's launch of electronic banking activities across its national borders fully aligns with possessing the appropriate systems to manage these banking risks.

**Section Three: Principles of Managing and Supervising E-Banking Risks**
The banking industry fundamentally relies on the art of risk management. Accordingly, measuring risks for the purposes of monitoring and controlling them is a primary role that new risk management departments in banks serve. These departments perform several essential functions, including:[20]
- Assisting in shaping a clear future vision, upon which the bank's plan and policy are based.
- Developing and enhancing a competitive advantage for the bank by controlling current and future costs that affect profitability.

[17]Monir Al-Nubihi&Mamdouh Al-Nubihi, previous reference, p.231.
[18] Abdel Razzaq Khalil &AhlamBouabdeli, The Arab Banking Industry and the Challenges of Basel II Agreement, paper presented at the International Finance Forum on the Issue of Emergence under Financial Globalization Pressures – The Case of the Algerian Economy, University of BadjiMokhtar, Annaba, 23–24 November 2004, p.10.
[19]Ahmed Saqr, previous reference, p.263.
[20]Monir Al-Janbihei, previous reference, p. 23.

- Estimating risks and hedging against them without negatively impacting the bank's profitability.
- Assisting in making pricing decisions.
- Developing the management of securities portfolios and working on diversifying those assets by improving the balance between risk and return.
- Helping the bank calculate the capital adequacy ratio according to the new Basel Committee proposals, which will represent a major obstacle for banks unable to measure and manage their risks scientifically. The Basel Committee's new requirements depend on the ability to measure, monitor, and control expected loss ratios, in addition to introducing new types of risks into proposed capital adequacy expenditures beyond what is currently included.

**Section Two: Principles of E-Banking Risk Management**
**Subsection one: Principles of E-Banking Risk Management**
Risk management includes evaluation, supervision, and monitoring as follows:
**Branch one: Risk Evaluation**– This involves:[21]
- Identifying the risks that the bank may face and assessing their potential impact on the bank.
- **Setting maximum limits** for the losses a bank can bear as a result of exposure to these risks.

**Branch Two: Risk Exposure Oversight**– which includes:[22]
**1. Implementation of security policies and procedures**:
- Verifying the identity of parties interacting with the systems / authentication.
- Ensuring that client messages are not altered during transmission through the channels.
- Ensuring the confidentiality of client transactions.
- Ensuring non-repudiation by the sender of the message.

**2.Additional security measures for issuing electronic money payment instruments**:
- Direct communication with the card issuer or central operator to prevent forgery.
- Monitoring individual transactions.
- Maintaining a centralized database to track money laundering activities.
- Ensuring security features in smart cards or other instruments, while setting a maximum storage limit on the card.
- Strengthening communication between different levels within the bank, from the Board of Directors to senior management, and among staff regarding system performance, with continuous employee training.
- Continuously providing and developing services.
- Establishing controls to limit risks when relying on external sources for technical support.

**Branch Three: Risk Monitoring** – involves selecting systems and procedures for internal and external auditing, as follows:[23]
**1.Conducting periodic system tests**, which include:
- Penetration testing aimed at identifying, isolating, and securing data flows within systems, and following procedures to protect the systems from unusual intrusion attempts.

[21]Youssef Messaadawi**,**Electronic Banks, paper presented at the Algerian Banking System and Economic Transformations Forum – Reality and Challenges, Faculty of Humanities and Social Sciences, Chlef, Algeria, December 14–15, 2004, pp. 227–228.
[22]Abdelrazak Khalil &HamzaTabi, previous reference, p.8.
[23]Monir Al-Janbihi**,**previous reference, p.24.

- **Conduct periodic system reviews:** to ensure the effectiveness of security measures and verify their consistency with established security policies and procedures.

**2.Internal and external audit procedures:** Internal and external audits contribute to identifying vulnerabilities and inefficiencies, reducing risk levels, and ensuring that the bank has developed policies and procedures and adheres to them.

**Subsection two: Supervision of Electronic Banking Risks**

The Basel Committee has emphasized the role of supervisory authorities in promoting and encouraging practices aimed at risk management in banks, as well as addressing deficiencies in risk management tools, including capital adequacy and compliance with disclosure requirements. This also involves internal controls, such as internal regulations, reinforcing policies related to provisions, and so on. The Committee focuses on prudential supervisory oversight as a secondary axis (similar to capital adequacy and market discipline) for the proper implementation of Basel II. Supervisory authorities responsible for implementing Basel II standards are urged to monitor banks, detect deviations, and address deficiencies in risk management.[24]

When we talk about bank supervision, we refer to banking supervision, which is exercised by external authorities under the central bank or the country's monetary authority. These supervisory authorities monitor banks' compliance with directives issued by the central bank and its affiliates and address recorded violations according to the law or regulations. They also engage in dialogue with banks to resolve issues that impede the proper functioning of the banking institution, limit the effectiveness of the supervisory committee, or address any shortcomings in prudential regulation caused by the banking environment. Appropriate and timely corrective measures are then taken. For example, the supervisory authority may adopt a strategy, after assessing financial needs to face risks, that focuses on banks with a specific risk profile, those occupying sensitive positions, or those engaged in important national economic activities.[25]

Among the instructions issued to a bank or banking organization under banking supervision:

**A. Policy formulation and implementation of procedures:** Supervisory authorities issue regulations that govern the policies adopted by bank management to cover the risks of its activities. They then verify the bank's compliance with these requirements. One of the most important practices required by security policies is to prepare a comprehensive program or update the current one, taking into account new electronic banking operations. The program should specify responsibilities and tasks for all parties and outline measures the bank will take in case of a security breach. This includes, as part of the remediation arrangements, estimating the cost of a breach and regularly reporting to the board of directors the risk levels resulting from these activities.[26]

**b. Information Density and Flow Channels:** Regulatory authorities assess the information systems and reporting or documentation systems within a banking institution to identify vulnerabilities that may distort the performance of tasks assigned to senior and executive management or lead to deviations in decision-making.

[24] Ibrahim Al-Karsana, Fundamental and Contemporary Frameworks in Bank Supervision and Risk Management, Arab Monetary Fund, Abu Dhabi, March 2006, p.47.
[25] Abdel Razak Khalil &AhlamBouabdelli, previously cited reference, p.13.
[26] Ibrahim Al-Karsana, previously cited reference, p.48.

**c. Conflicts Among Related Parties:** As part of governance requirements, i.e., the sound management of banks, regulatory authorities must support the bank in managing relationships with related parties by clarifying each party's obligations to ensure their rights, avoiding conflicts of interest, and directing decisions—especially strategic ones—away from personal agendas. This applies to relationships among the board of directors, major shareholders, borrowers, executive management, and internal and external auditors.

**d. Role of the Board of Directors and Its Responsibilities Toward Regulatory Authorities:** The primary responsibility for managing the bank rests with the board of directors. Its tasks include setting policies, approving systems, ensuring their proper implementation, and safeguarding the rights of depositors and the bank's assets. Consequently, the board is accountable to regulatory authorities for the bank's performance and results, including the soundness of its financial position and the transparency of information reported to regulators. This includes notifying regulators of candidates for membership on the board or executive management. The board must approve the bank's strategy for providing electronic banking services and endorse executive management policies for risk management and internal control evaluation through specialized committees under its authority.[27]

**e. Role of Executive Management and Its Responsibilities Toward Regulatory Authorities:** Regulatory authorities impose conditions on the human resources responsible for executive management, including practical competence, educational qualifications, good reputation, relevant experience, integrity, and absence of a criminal record. Authorities also impose requirements on banks to ensure that executive management conducts the bank's affairs according to the policies set by the board, while complying with all applicable laws. This includes defining the relationship between executive management and inspectors appointed by regulatory authorities, as well as providing prudential and statistical reports required by the board or regulators, among other obligations.[28]

**H. Guiding the Work of Internal and External Auditors:**

Supervisory authorities should encourage banks—through standards issued regarding internal and external auditing—to regulate the appointment of auditors, their responsibilities (professional, civil, and criminal), and their relationships with supervisory authorities. This framework should ensure neutrality and objectivity by making the audit department accountable to the board of directors and guaranteeing the auditor's independence in performing their duties, free from interference by bank management or pressure from shareholders.

Although laws generally require the appointment of one or more external auditors for institutions, in the banking sector the appointment must obtain the approval of the competent supervisory authority in addition to the decision of the general assembly. Supervisory authorities also have the right to request any data or clarifications from the auditor and may assign them tasks deemed necessary for supervisory purposes concerning the relevant bank.

At the same time, the auditor may refer to the supervisory authorities when required for the performance of their duties.

In all cases, the Basel Committee calls for national legislation to grant supervisory authorities an adequate degree of independence, as well as sufficient financial, human, and technical resources to perform their duties effectively.

[27]Abdel Razzaq Khalil &HamzaTabi**,**previously cited reference, p. 8.
[28]Ahmed Safar, previously cited reference, p. 235.

The purpose of assigning banking supervision to specific bodies affiliated with the central bank or monetary authority in most countries is to prevent conflicts between banking supervision and monetary policy that could negatively affect the national economy. Establishing such supervisory bodies also reduces the burden on the central bank in overseeing banking activities, allowing it instead to rely on evaluations prepared by supervisory committees to formulate appropriate guidance for the banking system.[29]

**Conclusion**

The study demonstrates that electronic banking has become one of the most significant manifestations of digital transformation in the banking sector, due to its contribution to accelerating transactions, improving service quality, and expanding access to financial services. However, this technological advancement has been accompanied by an increase in electronic risks associated with the use of digital platforms, making the management of e-banking risks a necessary requirement to ensure the security and stability of banking systems.

The study concluded that the effectiveness of e-banking risk management largely depends on banks adopting a set of organizational and technical principles and procedures, most notably the development of banking governance systems, the strengthening of cybersecurity infrastructure, and the continuous implementation of internal control and risk management standards. The findings also revealed that compliance with international information security standards contributes significantly to reducing cyber threats and enhancing the reliability of digital banking services.

Furthermore, the study highlighted the crucial role of banking governance in improving the effectiveness of electronic risk management through defining supervisory responsibilities, ensuring compliance with laws and regulations, and achieving integration among various internal control mechanisms. In addition, investing in cyber security systems and continuously updating security technologies are among the most effective means of combating cyber attacks and reducing risks related to hacking and electronic fraud.

On the other hand, the study confirmed that the success of electronic banking does not solely depend on technological advancement, but also on the level of digital awareness among employees and customers. Spreading digital culture and providing continuous training contribute to reducing human errors and strengthening confidence in electronic banking services.

The study also concluded that banking institutions still face several challenges in managing e-banking risks, most notably the continuous evolution of cyber threats, the high cost of technological protection systems, the lack of specialized expertise in certain banking environments, as well as legal and regulatory challenges related to data protection and privacy.

Based on the findings, the study proposes several recommendations, including:

Enhancing investment in cyber security technologies and regularly updating protection systems.

- Developing effective policies for managing electronic risks in accordance with international standards.
- Supporting training and capacity-building programs in digital security for banking sector employees.
- Promoting digital banking awareness among customers to reduce the risks of electronic fraud.
- Strengthening the role of regulatory authorities in monitoring banks' compliance with cyber security and risk management procedures.

[29]Abdel Razzaq Khalil &HamzaTabi**,**op. cit., p. 8.

In conclusion, achieving a secure and efficient electronic banking environment requires integrated efforts among banking institutions, regulatory bodies, and technological stakeholders in order to maximize the benefits of digital transformation while minimizing its risks, thereby enhancing trust and stability within the digital financial system.

**Bibliography**

1. Amine Tarazi, Banking Risk, Financial Deregulation, and Prudential Regulations, PUF, Paris, 1996
2. Brish Abdelkader, Banking Risk Management According to Basel II and III Regulations and the Requirements for Achieving Financial and Global Stability after the Global Financial Crisis, Journal of Humanities, Issue 29, Mohamed Khider University, Biskra, 2013.
3. Bakhtiar Saber Bayez Hussein, The Bank's Responsibility in Documentary Credit and the Risks it Faces, Dar Shatat for Publishing and Software, Egypt, 2010.
4. MedhatSadiq, Banking Tools and Techniques, Gharib Publishing and Distribution, Cairo, 2001.
5. Tarek Mohamed Khalil Al-Araj, Factors Affecting the Choice of Types of Services and Channels Offered by Electronic Banks – An Analytical Study of the Opinions of a Sample of Customers of Qatari Banks, Doctoral Dissertation.
6. Ali Badran, Modern Management of Banking Risks under Basel II, Al-Muhasib Al-Jaz [The Accountant], Chapter Three, Issue 23, Basel, 2005.
7. ChoulChahra&Madoukh Magda, Electronic Banking: Its Nature, Risks, and Protection, paper presented at Banking System in the Third Millennium: Competition, Risks, Technologies, University of Jijel, Algeria, June 6–7, 2005.
8. Abdel Razzaq Khalil &AhlamBouabdeli, The Arab Banking Industry and the Challenges of Basel II Agreement, paper presented at the International Finance Forum on the Issue of Emergence under Financial Globalization Pressures – The Case of the Algerian Economy, University of BadjiMokhtar, Annaba, 23–24 November 2004.
9. Youssef Messaadawi,Electronic Banks, paper presented at the Algerian Banking System and Economic Transformations Forum – Reality and Challenges, Faculty of Humanities and Social Sciences, Chlef, Algeria, December 14–15, 2004, pp. 227–228.
10. Ibrahim Al-Karsana, Fundamental and Contemporary Frameworks in Bank Supervision and Risk Management, Arab Monetary Fund, Abu Dhabi, March 2006.