

E-Banking Risk Management Strategies in Light of the Recommendations of the Basel Committee on Banking Supervision

KHELIFA Mounia, DERRADJI Aissa

university of khemis Miliana(Algeria),), m.khelifa@univ-dbkm.dz
derradji.aissa@univ-tissemsilt.dz

Received: 15./11/2025

Accepted: 12/01/2026

Published:26./01/2026

Abstract:

This study aims to analyse effective strategies for managing banking risks within the context of digital transformation, with a specific focus on e-banking. Employing a descriptive-analytical approach, the research identifies and examines the various types of risks emerging from digitization, alongside methods to address them.

The findings reveal that alongside traditional risks, new and complex challenges have arisen, including cybersecurity threats, technology fraud, and data privacy and compliance risks. The results clearly indicate that the success and resilience of banks in the digital age depend on the strategic integration of robust traditional risk management methods with modern, technology-driven strategies. Furthermore, the study underscores the continued necessity of adhering to Basel principles to ensure adequate capital adequacy and robust operational risk management. It concludes that a holistic model, combining proven risk fundamentals with innovative regulatory technology, is essential for ensuring the banking sector's stability and sustainability against an evolving digital threat landscape.

Keywords: E-banking, Risk Management, Digital Banks, Basel Principles, Operational Risks

1. INTRODUCTION

The global banking sector is witnessing a radical transformation driven by the digital revolution, where e-banking has become an inevitable reality. This transformation is accompanied by new and complex risks that threaten the security and integrity of financial systems. Therefore, there is an urgent need to analyse effective strategies for managing these risks within the evolving digital environment and in accordance with the Basel Committee on Banking Supervision's regulations.

Through this study, we seek to evaluate these strategies using the descriptive-analytical approach to identify optimal coping mechanisms. We attempt to present an integrated framework that enables banks to maximize the benefits of digital opportunities while mitigating the associated challenges and proposing practical frameworks for their management, based on the guiding principles of the Basel Committee on Banking Supervision.

2. The Theoretical Framework of E-Banking:

2.1 The Concept of E-Banking

E-banking, also known as electronic banking, is comprehensively defined as the automated delivery of traditional and innovative financial services directly to customers through open or closed electronic communication channels and their equivalents. This revolutionary concept represents a fundamental shift from the physical brick-and-mortar model, enabling users to conduct a vast array of banking transactions remotely and conveniently.

The evolution of e-banking has been profound. It began with foundational services such as telephone banking and Automated Teller Machines (ATMs), which introduced the concept of self-service for basic tasks like balance inquiries and cash withdrawals. This first wave of digitization gradually expanded to include more complex services via dedicated dial-up networks.

The most significant transformation occurred with the advent of the internet and mobile technology. This gave rise to comprehensive online banking platforms accessible via web browsers and, subsequently, sophisticated mobile banking applications. Today, e-banking encompasses a

***E-Banking Risk Management Strategies in Light of the Recommendations of
the Basel Committee on Banking Supervision***

full suite of services, including real-time fund transfers, bill payments, loan applications, investment management, and personalized financial analytics, all accessible 24/7 from a customer's personal device. This continuous innovation has fundamentally reshaped the customer experience, emphasizing speed, accessibility, and customization in the financial sector.

2.2 The Historical Development of E-Banking

The historical development of e-banking can be traced chronologically as follows: (Supervision, 2020, p. 27)

2.2.1 The Seventies: The Beginning of Online Banking Services:

This period witnessed the first beginnings of e-banking with the emergence of "online" systems. These services relied on customers connecting to the bank via specialized terminal devices or via telephone using button tones. They allowed users to perform simple inquiries on their accounts, such as checking balances and recent transactions. This stage represented the foundation stone for remote banking services, transforming banks from purely physical entities into services accessible electronically.

2.2.2 The Eighties: The Proliferation of ATMs:

Automated Teller Machines (ATMs) became the cornerstone of e-banking during this period, changing the pattern of customer interaction with their money. Banking services were no longer limited to official working hours but became available 24/7. These machines provided basic services such as cash withdrawal, deposit, fund transfers, and balance inquiries. This proliferation had a significant social and cultural impact, reinforcing the idea of the "bank that never sleeps" and expanding the geographical scope of banking services.

2.2.3 The Nineties: The Internet Revolution and Web Expansion:

With the global spread of the Internet, e-banking entered its golden age with the emergence of the first online banks. This allowed customers to access their accounts and conduct complex transactions from anywhere with an Internet connection, such as transfers between accounts and bill payments. This period witnessed a fundamental shift from basic electronic services to an integrated banking model via digital platforms. New risks also began to appear, necessitating the development of the first cybersecurity systems to protect online transactions.

2.2.4 The Third Millennium: Multi-Channel and Mobile Banking:

This stage was characterized by the spread of banking services across all digital media, especially mobile phones and smart applications. Access to services was no longer exclusive to computers but became available in the user's pocket anytime, anywhere. This led to the emergence of advanced concepts such as e-wallets, mobile payments, and fully digital banks. This revolution transformed banks from physical entities into digital platforms offering a seamless and personalized user experience, focusing on speed, convenience, and accessibility.

2.3 Advantages of E-Banking:

The most important advantages of e-banking include the following (Bank for International settlements, 2020,p 27) :

- Reduction of operational costs for banks;
- Expansion of the scope of banking services;
- Improvement of Customer experience with banks;
- Increased efficiency of banking services performance;
- Access to new markets through electronic outlets and networks.

2.4 E-Banking Channels:

Electronic banking services are delivered through a number of equivalents and means, the most important of which are:

- Automated Teller Machines (ATMs);
- Smartphone Banking;
- Internet Banking;
- Laptop Banking;
- Electronic Point of Sale (POS) terminals;
- Automated payment and settlement systems.

2.5 Risks of E-Banking:

The following outlines the most important risks facing e-banking:

2.5 1. Strategic Risks:

These risks arise from top management's erroneous decisions regarding the development and implementation of e-banking strategies. They include (Bessis & John Wiley and Sons, 2015, p. 123):

- Misjudging market needs;

E-Banking Risk Management Strategies in Light of the Recommendations of the Basel Committee on Banking Supervision

- Inadequate planning of financial resources (loans and deposits);
- Failure to keep pace with technological developments;

2.5 2. Operational Risks:

These are considered the most associated with e-banking and arise from:

- Security breaches;
- Technical system failures;
- Human errors;
- Inadequate internal control oversight.

2.5 3. Reputational Risks:

Result from:

- Frequent service interruption ;
- Security breaches;
- Poor service quality;
- Failure to fulfil marketing promises;
- Rumors that may affect some banks and spill over to others.

2.5 4. Legal and Compliance Risks (Prepared by Frank Adelmann, 2020, p. 57):

Include:

- Banks' non-compliance with data and information protection laws;
- Money laundering risks;
- Lack of clarity in the legal framework for electronic transactions;
- Issues related to jurisdiction in transactions.

2.5 5. Credit Risks in the Electronic Environment:

These refer to potential losses the bank may incur due to the inability of the customer or counterparty to fulfil their financial obligations on the agreed dates, within the context of services and products offered through digital channels. What distinguishes these risks in the electronic environment includes:

2.5 5.1 Lack of Physical Interaction: Difficulty in directly verifying the customer's identity and document authenticity, in addition to the inability to assess creditworthiness through traditional means (like personal interviews).

2.5 5.2 Speed in Granting Credit: Electronic banks rely on automated and

fast models for making loan or credit card granting decisions, which may increase the probability of error.

2.5 5.3 Potential for Electronic Fraud: Identity theft using stolen data, and the possibility of creating fake accounts for fraud.

2.5 5.4 Difficulty in Verifying Customer Nature: Attracting new customers from segments that may not have a traditional credit history (e.g., the digital generation, customers in remote areas).

The importance of these risks stems from the difficulty of assessing customers' creditworthiness remotely and the high probability of electronic fraud.

2.5 6. Liquidity Risks:

These are risks where the bank is unable to meet its short-term financial obligations when they fall due, because it cannot convert its assets into liquidity without significant losses, or sufficient cash is not readily available. They primarily arise from the following sources:

2.5 6.1 Mismatch between Maturity Dates and Deposit Terms: This is the root cause in the banking sector. Banks borrow short-term funds (deposits) and lend them as long-term loans. If all depositors demand their money at once, the bank cannot recall the long-term loans quickly.

2.5 6.2 Loss of Confidence: Any shock to confidence in the bank or the banking system as a whole leads customers to rush to withdraw their deposits simultaneously.

2.5 6.3 Systemic Financial Crises: Where liquidity sources dry up in the entire market, and no one finds a lender.

2.5 6.4 Poor Balance Sheet Management: Lack of an effective liquidity plan or sufficient diversification of funding sources.

The impact of liquidity risks is deepened in electronic banks, making them more acute due to:

2.5 6.5 Rapid Spread of Rumors and Loss of Confidence (Digital Reputation): In the digital age, a negative rumor about the bank can spread via social media or review platforms at an enormous speed. Even a minor technical glitch or security breach can lead to a wave of panic and an "electronic run" by depositors, who withdraw their money with a click of a button, in record time.

E-Banking Risk Management Strategies in Light of the Recommendations of the Basel Committee on Banking Supervision

2.5 6.6 Ease and Speed of Deposit Withdrawals (A Click Away): In traditional banks, withdrawing a large amount may require a branch visit and procedures that could slow the process. In electronic banks, a customer can transfer all their funds to another bank in minutes through an app on their phone. This extreme speed in capital movements reduces the time available for the bank to respond to a potential liquidity crisis.

2.5 6.7 Nature of the Customer Base: Electronic banks often attract customers from the "digital generation" or those seeking the best returns. These customers may be less loyal and more willing to transfer their funds merely upon the appearance of a better offer or the slightest doubt about the bank's operational stability.

2.5 6.8 Heavy Reliance on Short-Term Deposits: Many electronic banks promote high-yield savings accounts to attract customers. These deposits are mostly short-term and highly mobile, increasing the "instability" of the funding base (Lall, 2019).

2.5 6.9 Limited Asset Base (for Pure Electronic Banks): Many emerging electronic banks do not have great diversity in assets (like a diversified loan portfolio with graduated maturities). They may rely on investing deposits in specific liquid assets, reducing their flexibility in managing liquidity.

2.5 7. Interest Rate Risks in Electronic Banks:

Refer to potential losses resulting from unexpected fluctuations in interest rates, which affect the profit margins between lending and deposit rates. In the electronic environment, these risks are exacerbated due to several reasons, the most important of which are:

2.5 7.1 Intense Competition for Online Deposits: Given the availability of electronic networks, customers can easily compare interest rates between electronic banks in minutes, putting pressure on banks to raise deposit interest rates to attract customers, thus narrowing the interest rate spread between revenues and costs.

2.5 7.2 Rapid Transmission of Central Bank Decisions: Any change in official interest rates is instantly disseminated through digital platforms. Electronic banks do not have enough time to adjust their product structure or strategy, unlike traditional banks.

2.5 7.3 High Customer Sensitivity to Interest Rates: Customers of

electronic banks are often less loyal and more responsive to changes in rates. They can quickly withdraw and transfer their funds to a competitor offering a higher return, increasing deposit volatility and making liquidity and cost planning difficult.

2.5 7.4 Mismatch between Asset and Liability Maturities: Many electronic banks rely on short-term deposits (like online savings accounts) to finance long-term loans. If interest rates rise, they will have to pay higher rates on deposits while their revenues from loans remain fixed (if their rates are fixed), thus reducing profitability.

2.5 7.5 High Transparency and Instant Comparison: Specific websites provide the ability to compare prices, increasing customer awareness and accelerating the transfer of funds between banks, making the interest rate the primary factor in attracting customers, at the expense of other factors like services or reputation. (Settlements, High-level principles for digital transformation of financial institutions and for the digitalisation of financial services, 2023, p. 15)

2.5 7.6 Reliance on Standardized Products with Narrow Margins: Many digital banks offer simple products (savings accounts, personal loans) that are easily replicated by competitors, limiting their ability to create innovative products that achieve higher margins and reduce risks.

2.5 7.7 High Marketing Costs: Electronic banks, to attract customers in a crowded environment, are forced to spend large sums on digital marketing and promotional offers (like temporary high-interest periods). These costs may pressure profitability when interest rates return to normal levels.

2.5 7.8 Big Data and Inadequate Forecasting: Despite the availability of data, predictive models in electronic banks may not accurately predict customer behavior in a rapidly changing environment.

2.5 7.9 Regulatory Boundaries: Some emerging electronic banks may not have sufficient experience or advanced tools to manage interest rate risks with the same efficiency as major traditional banks.

2.5 8. Exchange Rate Risks in Electronic Banks:

These are represented by potential losses resulting from fluctuations in the exchange rates of foreign currencies dealt with by the electronic bank, which affect: (Settlements, High-level principles for digital

E-Banking Risk Management Strategies in Light of the Recommendations of the Basel Committee on Banking Supervision

transformation of financial institutions and for the digitalisation of financial services, 2023, p. 56)

- The value of assets and liabilities denominated in foreign currencies,
- Profit margins from international transactions,
- The bank's financial position when converting financial statements.

2.6 The most important sources of this type of risk in electronic banks include:

2.6.1 Cross-Border Cash Transactions:

- International customer transfers
- Global e-commerce payments
- Transactions in foreign currencies

2.6.2 Open Financial Positions for Electronic Financial Transactions:

- The gap between assets and liabilities in foreign currencies
- Customer positions not denominated in the local currency

2.6.3 Competitive Risks:

- Changes in exchange rates affect customers' ability to compete internationally
- Impact on the demand for international banking services

3. Risk Management Strategies in Electronic Banks and the Responsibility of Supervisory Bodies:

3.1. The General Framework for Risk Management:

The risk management process is based on four basic stages: (BCBS, 2003, p. 108)

3.1.1 Identifying the Nature of Risks: Recognizing all potential risks in their nature and type;

3.1.2 Measuring Risks: Developing quantitative and qualitative indicators to assess and measure the value of risks;

3.1.3 Treating Risks: Determining appropriate procedures and strategies to confront risks according to the defined stages and implementing them.

3.1.4 Monitoring and Follow-up: Continuous review of controls related to risk treatment and working on forecasting and early warning to hedge against or confront them.

3.2. Risk Management Mechanisms in Electronic Banks:

3.2.1. Managing Strategic E-Risks: Can be addressed through: (BCBS, Risk Management Principles for Electronic Banking and Electronic Money, 2003, p. 156)

- Conducting regular SWOT analysis;
- Ensuring the technology strategy aligns with the business strategy;
- Adopting effective management of organizational electronic change.

3.2.2. Managing Operational Risks: Electronic banks adopt some necessary procedures to manage their operational risks, the most important of which are:

- Developing strong information security systems;
- Implementing intrusion detection systems;
- Conducting regular penetration tests;
- Establishing business continuity plans;
- Training employees on cybersecurity.

3.2.3. Managing Reputational Risks: To avoid these risks, banks must adopt the following mechanisms:

- Developing an effective communication strategy to face crises;
- Transparency in dealing with customers through electronic means;
- Monitoring social media and electronic platforms;

Responding quickly to customer complaints and feedback raised electronically.

3.2.4. Managing Legal Risks: Electronic banks follow some procedures, the most important of which are:

- Establishing a specialized department for electronic compliance;
- Periodic review of banking regulations and laws and adjusting them to align with technological and electronic developments;
- Documenting all electronic transactions and ensuring their encryption and protection with effective firewalls and antivirus software;

3.2.5. Managing Financial Risks (Linda Allen, 22 April 2025, p. 238): This type of risk can be managed through the following mechanisms:

- Developing advanced electronic programs for credit management;

E-Banking Risk Management Strategies in Light of the Recommendations of the Basel Committee on Banking Supervision

- Improving treasury and liquidity management;
- Diversifying the portfolio of financial products and banking services;
- Using electronic tools for financial hedging.
- Adopting early warning mechanisms for risks electronically;
- Developing supervision and auditing procedures for electronic services.

3.2.6. Managing Liquidity Risks in Electronic Banks: To manage this type of risk, banks must adopt the following methods:

- Big Data and Advanced Analytics;
- Necessity of collecting and analyzing customer data in real-time;
- Developing programs to predict withdrawal behavior based on accurate predictive models to anticipate deposit withdrawal patterns.
- Maintaining a relatively higher liquidity reserve without imposing a significant burden on profitability.
- Having the ability to quickly adjust deposit interest rates via the application to attract new deposits or slow withdrawals, in response to market conditions.

3.3. The Responsibility of Supervisory Bodies in Managing E-Banking Risks:

3.3.1. Responsibilities of Senior Management:

- Setting clear risk management policies
- Allocating sufficient resources
- Periodic review of the efficiency of risk management systems
- Ensuring activities align with the overall strategy

3.3.2. Role of the Internal Audit Committee:

- Reviewing the effectiveness of internal control oversight
- Assessing the adequacy of risk management policies
- Reviewing periodic reports on cybersecurity incidents
- Evaluating the extent of compliance with regulatory statutes

4.The Fourth Axis: Principles of the International Basel Committee for Managing E-Banking Risks

The Basel Committee on Banking Supervision has placed great importance on services provided through electronic media, calling for the

necessity of managing their risks due to the potential for crises that could spill over into banking and financial systems given their global interconnectedness. Among the most important of these recommendations are the following: (Sauvageot, 2017, p. 104)

4.1. Establishing an effective Electronic risk management function:

Senior management in the bank must develop and implement an integrated framework for managing e-banking risks. This includes identifying, analysing, and assessing all risks associated with new and existing electronic services. These policies must be comprehensive, clear, and commensurate with the size and technical complexity of the bank's activities. The goal is to build a proactive strategy that prevents problems before they occur rather than merely reacting to them.

4.2. Conducting independent audits of electronic risks:

This principle requires the existence of independent internal and external audit processes to assess the effectiveness of information security controls and risk management. The audit team must have sufficient technical expertise to understand the complexities of the electronic environment. These periodic reviews aim to uncover gaps and weaknesses in systems and processes. Results and recommendations are presented directly to senior management for necessary corrective actions.

4.3. Transparency and Disclosure of Electronic Data and Information:

The bank must provide its customers with clear and sufficient information about the nature of electronic services and the associated risks. This includes disclosing terms of service, the customer's responsibilities in maintaining account security, and how to report suspicious transactions. This transparency aims to empower customers and build trust, ensuring their full understanding of their rights and duties in the digital space.

4.4. Secure Customer Authentication:

This principle focuses on the importance of verifying user identities in a robust manner to ensure that access to accounts and services is restricted to authorized persons only. Authentication methods should go beyond simple passwords to include multiple factors like one-time passwords (OTP) or biometrics. This is a key defensive barrier against identity theft and unauthorized access to accounts. (Dapp, 2019, p. 66)

4.5. Non-Repudiation and Integrity of Electronic Transactions:

Aims to ensure that no party to an electronic transaction (the bank or the customer) can deny having conducted it later. This is achieved through mechanisms such as electronic signatures, digital certificates, and encryption. It also ensures the integrity and confidentiality of transaction data while in transit over public networks. This provides the legal basis for adjudicating any disputes that may arise regarding the validity of the transaction.

4.6. Controls for Responsibilities and Authorities for Electronic Processes:

This refers to the necessity of segregating duties and responsibilities within the bank to prevent the concentration of powers in the hands of a single individual, thereby reducing the risks of internal fraud or errors. Employees should be granted the minimum necessary privileges only to perform their tasks. All sensitive activities are recorded in non-tamperable audit logs to ensure the traceability of any action to its perpetrator.

4.7. Ensuring Electronic Data Security and Confidentiality:

Mandates the protection of customers' confidential information and sensitive financial data from unauthorized access, disclosure, or modification. This applies to data "in transit" over the Internet and "at rest" on the bank's servers. This is achieved primarily through the use of strong encryption technologies, firewalls, and intrusion detection systems. This principle is fundamental for compliance with data protection laws and maintaining customer trust.

4.8. Business Continuity and Electronic Disaster Recovery Planning:

This principle requires the electronic bank to have comprehensive plans to ensure the continuity of electronic service delivery in the event of a major technical failure, natural disaster, or cyber-attack. These plans include backup systems, alternative data centers, and detailed recovery procedures. These plans must be tested regularly to confirm their effectiveness and the bank's ability to resume operations as soon as possible.

4.9. Rapid Incident Handling and Response:

Mandates the establishment of a specialized incident response team equipped with the necessary resources and authorities. The team must have predefined procedures for detecting, containing, eradicating, and recovering

from incidents. This includes analysing the root cause of any incident and implementing measures to prevent its recurrence. Rapid reporting of incidents to regulatory authorities and customers (where applicable) is an essential part of this principle.

4.10. Management of Outsourcing Risks:

When a bank uses an external service provider (such as a cloud provider or software developer), the ultimate responsibility for managing the risks associated with that service remains with the bank. Service Level Agreements (SLAs) must include strict terms for security, confidentiality, and business continuity plans. The bank must conduct periodic assessments to ensure the external service provider's compliance with agreed-upon security standards and policies. (BCBS, Principles for the Sound Management of Operational Risk, 2021, p. 76)

4.11. Legal Management of Electronic Risks

The bank must ensure that all e-banking activities comply with relevant local and international laws and regulations. This includes data protection laws, banking regulations, and anti-money laundering laws. The legal framework must cover the validity of electronic transactions and the rights and responsibilities of all parties. The goal is to reduce exposure to legal risks and lawsuits.

4.12. Risk Disclosure via Electronic Channels:

All information related to products and services offered through electronic channels must be accurate, clear, updated, and easily accessible to customers. This disclosure must include any fees, conditions, or potential risks associated with the service. This principle prevents deceptive practices and ensures that the bank's customers are sufficiently informed to make sound financial decisions. (Settlements, Core Principles for Effective Banking Supervision, 2012, p. 45)

4.13. Privacy and Electronic Data Protection:

The bank must have written and transparent policies on how it collects, uses, stores, and protects customers' personal data. Customer consent must be obtained when necessary, and they must have rights to access and correct their data. Compliance with privacy laws like the GDPR is crucial not only to avoid fines but also to maintain the bank's reputation and customer trust.

4.14. Reporting Suspicious Electronic Activities:

Banks must establish effective systems to monitor electronic transactions to detect unusual or suspicious activities that may indicate money laundering, terrorist financing, or fraud. Upon detecting suspicious activity, the bank must report it immediately to the competent authorities according to local laws. This principle contributes to protecting the entire financial system from use by criminal elements.

5. Conclusion:

Through this study, we have clarified the necessity of adopting advanced digital mechanisms for managing e-banking risks, by developing an integrated framework that combines traditional and modern methods that align with the specific nature of this type of banking service. The study also emphasizes the importance of adhering to Basel principles for banking supervision and principles of good governance, with a focus on operational, technical, cyber risks, and regulatory compliance.

We also concluded on the necessity of assessing electronic risks and integrating traditional and digital channels as a means to enhance rapid and efficient risk response, while applying penetration tests and assessing the impact of digital systems on the supply chain. And developing an institutional plan that includes SWOT analysis of digital risks, and reinforcing continuous awareness and training for employees on security policies and compliance

5.1. The Main Findings of the Study:

Through this study, we can conclude fundamental results, the most important of which are:

- **Nature of Risks:** In the context of electronic banks, risks are no longer limited to credit or liquidity risks; rather, operational risks and cybersecurity are now at the forefront, followed by reputational risks.
- **Integration:** It is not possible to rely solely on traditional risk management strategies. They must be integrated with modern strategies focusing on advanced technologies such as artificial intelligence and big data for monitoring and early warning.
- **Compliance with International Frameworks:** The results confirm that the Basel principles for managing e-banking risks constitute a fundamental framework indispensable for any bank seeking to build

an effective risk management system.

- **Centrality of the Human Element and Technology:** The success of the strategy depends on balancing investment in advanced security technologies with building a risk-aware organizational culture and continuously training human resources.

5.2. Recommendations:

In light of the previous results, the study concludes that risk management in the digital age is a dynamic and continuous process, not a routine activity. Accordingly, we present the following recommendations:

- **Adopting an Integrated Risk Management Model:** Integrating digital risk management into all bank operations and stages of new product development.
- **Strengthening Cybersecurity Infrastructure:** Investing in the latest protection technologies, encryption, and intrusion detection systems.
- **Continuous Assessment of Third-Party Risks:** Establishing strict frameworks for assessing and monitoring external technology service providers.
- **Enhancing Transparency and Disclosure:** To build customer trust and educate them about the risks of electronic operations and protection methods.
- **Continuous Compliance with International Principles:** Adopting Basel principles as a minimum standard, while keeping pace with any updates or new guidelines issued by regulatory bodies.
- **Necessity of Using Advanced Modeling and Simulation:** Through the use of techniques like **stress testing** and **repricing gap analysis** to measure the impact of price fluctuations.
- **Leveraging Big Data and Artificial Intelligence** to predict customer behavior and their response to changes.
- **Working on Balancing Assets and Liabilities:** Attempting to achieve a balance between the maturities and sizes of interest rate-sensitive assets and liabilities, and developing innovative financial products with flexible characteristics that help manage this gap.
- **Using Financial Derivatives:** Resorting to **interest rate swaps** and **forward agreements** to hedge against undesirable fluctuations.

E-Banking Risk Management Strategies in Light of the Recommendations of the Basel Committee on Banking Supervision

- **Adopting a Dynamic Pricing Strategy:** Due to the digital nature, interest rates on deposits and loans can be adjusted quickly in response to market conditions. And applying a **dynamic discovery model** to find the optimal price that balances attractiveness to customers and profitability for the bank.
- **Necessity of Enhancing Transparency and Managing Customer**
- **Expectations:** Through clear communication with customers about pricing policies and the mechanism for adjusting interest rates, in addition to building trust and reducing the phenomenon of customers suddenly switching due to any minor change in prices.

6. Bibliography List :

1. Basel Committee on Banking Supervision. "Risk Management Principles for Electronic Banking". (2020)
2. Bessis, J. "Risk Management in Banking". John Wiley & Sons. (2015).
3. Lall, S. "Cyber Risk Management in Financial Institutions". Journal of Financial Régulation. (2020).
4. Risk Management Principles for Electronic Banking and Electronic Money. (BCBS). 2003.
5. Power, M. "Risk Management in Digital Banking". Oxford University Press. 2018.
6. The Oxford Handbook of Banking: 4th Edition (4th edn)
7. Allen N. Berger , March 2025
8. Dapp, Thomas F. Digital Banking and the Challenges of Cybersecurity: Concepts, Solutions, and Strategies for the Financial Services Industry (2019)
9. Core Principles for Effective Banking Supervision Bank for International Settlements (BIS) - Updated version (2012)
10. Principles for the Sound Management of Opérationnel Risk. (BCBS). 2021.
11. High-level Principles for digital transformation of Financial institutions and for the digitalisation of Financial services. Bank for International Settlements 2023