

## **Artificial Intelligence in the Banking Sector: Navigating Risks and Their Management — Pioneering Intelligent Models to Mitigate Banking Risks**

GUERFI Omar <sup>1</sup>/ Faculty of Economics and Commerce - Abd Elhafid Boussouf - University of Mila, Algeria, [omar.guerfi@centre-univ-mila.dz](mailto:omar.guerfi@centre-univ-mila.dz)

Received: 01/05/2025

Accepted: 04/12/2025

Published: 29-12-2025

### **Abstract:**

*The increased reliance on artificial intelligence (AI) in the banking sector has resulted in several significant challenges. Advanced technologies, such as deep fakes, can be exploited to carry out sophisticated fraud against banking systems, resulting in serious threats to financial stability. Similarly, biased data within machine learning algorithms may lead to discriminatory credit decisions that would, hence, necessitate periodic audits and comprehensive regulatory controls.*

*This study aims to highlight the role of AI as a fundamental tool in risk management and fraud prevention. The adoption of real-time fraud detection systems, supported by deep learning models and real-time analytics, has contributed to a measurable reduction in fraudulent financial losses. Moreover, AI-based systems have promoted regulatory compliance by automating the analysis of regulatory texts, allowing for more efficient and accurate adherence to legal standards across the banking sector.*

**Keywords:** Artificial Intelligence, Banking, Cyber-security, Governance, Fraud Detection

**Jel Classification Codes :** C45; G21; G28; G34; K42.

---

### **résumé:**

*L'adoption croissante de l'intelligence artificielle (IA) dans le secteur bancaire engendre des défis majeurs. Des technologies avancées, telles que les deepfakes, peuvent être exploitées pour orchestrer des fraudes sophistiquées à l'encontre des systèmes bancaires, menaçant ainsi la stabilité financière. De plus, l'utilisation de données biaisées dans les algorithmes d'apprentissage automatique peut entraîner des décisions de crédit discriminatoires, rendant indispensables des audits périodiques et des contrôles réglementaires rigoureux.*

*Cette étude vise à mettre en lumière le rôle fondamental de l'IA dans la gestion des risques et la prévention de la fraude. L'intégration de systèmes de détection de fraude en temps réel, soutenus par des modèles d'apprentissage profond et des analyses instantanées, a permis une réduction significative des pertes financières liées à la fraude. Par ailleurs, les systèmes basés sur l'IA ont favorisé la conformité réglementaire en automatisant l'analyse des textes législatifs, assurant ainsi une adhésion plus efficace et précise aux normes juridiques dans l'ensemble du secteur bancaire.*

**Mots-clés:** Intelligence artificielle, Banque, Cyber-sécurité, Gouvernance, Détection de fraude

**Jel Classification Codes :** C45; G21; G28; G34; K42.

<sup>1</sup>. Corresponding author: Omar Guerfi, e-mail address: [omar.guerfi@centre-univ-mila.dz](mailto:omar.guerfi@centre-univ-mila.dz)



## ***I. Introduction***

This paper purports to investigate the diverse risks associated with the implementation of artificial intelligence (AI) in the banking sector. The study highlights the cyber threats, predictive errors, and algorithmic biases. In addition to identifying these risks, the study offers a set of strategies and solutions to protect against these risks. Moreover, the work explores selected AI models deployed to mitigate banking risks, including fraud detection models, credit rating assessments, and automated compliance systems.

The primary problem addressed is how to balance between leveraging the advanced capabilities of AI and ensuring the security and stability of banking systems. Sub-problems are related to examine the technical and regulatory aspects of this process. Therefore, the study attempts to highlight AI related risks in banking and how AI can be used protect against them through the presentation of practical and effective risk management models.

Therefore, the central research question addressed in this study is:  
How can banking institutions leverage artificial intelligence (AI) capabilities to enhance risk management capabilities?

### **Sub-questions:**

- How can artificial intelligence techniques, such as deep learning and real-time analytics, enhance banks' capabilities for early detection of financial fraud?
- How effective are artificial intelligence systems in promoting regulatory compliance and reducing biased credit decisions within banking institutions?

### **Hypotheses:**

- The adoption of artificial intelligence systems for real-time fraud detection significantly reduces financial losses resulting from fraudulent activities in banks.
- The use of artificial intelligence in analyzing regulatory texts and credit decisions contributes to enhancing compliance with legal standards and reducing bias in loan granting.

### **Methodology:**

- The study is descriptive and analytical in nature, relying on a review of scientific literature, case studies of banks that implement AI systems for fraud detection and regulatory compliance, and supporting findings with real-world examples and comparative studies between banks.
- Data analysis involves examining outputs from intelligent models (Deep Learning Models) and analyzing internal audit and regulatory compliance reports of banks.

## ***II. Literature review***

1. Artificial intelligence (AI) is as a branch of computer science that focuses on developing systems, programs, and algorithms capable of performing tasks that typically require human intelligence and acting in ways similar to the human mind, such as logical reasoning, creativity, and planning. This includes the ability to learn from data and past experiences, understand natural language, recognize sounds and images, make decisions,



and provide intelligent solutions to problems presented to it in performing specific tasks. (Russell & Norvig, 2020, P1 )

### ***II.1. Underlying Motivations for the Growing Interest in Artificial Intelligence***

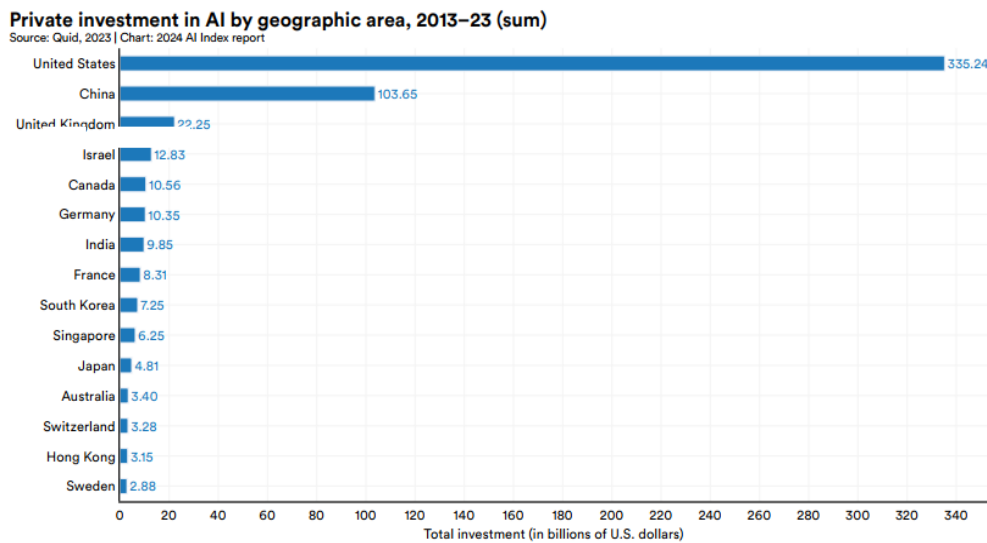
Several factors contribute to the growing interest in AI. These factors are listed below:

- The potential for self-education and self-development through AI programs, such as machine learning, logic, self-correction, and self-programming.
- Artificial intelligence aids in alleviating the burdens and risks associated with human labor, particularly in areas such as exploration. The education system is expected to undergo both conceptual and structural changes as a result of implementing the principles of the Fourth Industrial Revolution, with focus on sensory learning to meet the evolving demands of the industrial and AI driven sectors.
- Artificial intelligence has the potential to create new job opportunities, deliver services at reduced costs, and contribute to maintaining security. Additionally, it provides mechanisms and solutions to address challenges such as cybercrime.
- The information and knowledge storage associated with artificial intelligence enable organizations to protect institutional knowledge from loss due to employee turnover, including resignation, transfer, or death.
- AI enables the establishment of mechanisms not subject to human emotions such as anxiety, fatigue, or exhaustion, especially when it comes to strenuous work that poses physical and mental risks. It also generates and finds solutions to complex problems, facilitates their timely analysis and resolution (Majid Ahmed , 2018, p. 18)

Driven by ambitious plans for AI adoption, most financial institutions, mainly banks, are expected to increase their investment in artificial intelligence in the short term. This trend is particularly evident among companies that already spend more than 20% of their research and development resources on AI, with more than half of them anticipating a substantial increase in investment in the next two years (Cambridge Centre for Alternative Finance, & World Economic Forum, 2020, p. 26).

When aggregating private investment in artificial intelligence over the period from 2013 to 2023, the United States maintains its lead with \$335.2 billion, followed by China with \$103.7 billion, and then the United Kingdom with \$22.3 billion (Figure 01) (Artificial Intelligence Index Report, 2024, p. 247).

**Figure No. (01): Private investment in artificial intelligence by geographic region, 2013–2023 (total)**



**Source :** (Artificial Intelligence Index Report, 2024, p. 19)

**II.2. Applications of Artificial Intelligence in the Banking Sector :**

AI has a wide range of applications, including:

- Customer Service: AI powered Intelligent robots and virtual assistants have significantly revolutionized customer service within the banking and financial sectors. These systems are capable of answering customer inquiries, solving problems, and providing recommendations, thereby enhancing the overall quality and efficiency of customer assistance. Their availability around the clock and ability to manage multiple customer conversations simultaneously contribute to an improved customer experience and expedited service delivery (Jain, R, 2023, pp. 1-4).

- Applications in Banking Marketing: Big data and AI play a pivotal role in modern banking marketing by enabling the analysis and classification of user-generated data. By integrating relevant information, such as consumption preferences, financial status, and behavioral patterns, AI driven platforms can accurately identify customer needs, create customer profiles, anticipate customer desires, match and push personalized products, and generate advertising texts. As a result, advertisers and marketers are increasingly recognizing the advantages of intelligent marketing and are investing in a variety of disciplines to build sophisticated systems. One example includes the intelligent design of the marketing-oriented payment architecture (Ridzuan et al, 2024, pp. 96-97).

- Fraud Detection: Fraud detection is a critical area within the financial sector, particularly in banking, that relies heavily on artificial intelligence (AI). AI systems have become increasingly prominent in detecting fraudulent activities and deception by customers. One early and successful application of data



analytics techniques in the banking sector is the ico-Falcon fraud assessment system, which utilizes a neural network, to deploy advanced AI systems based on deep learning (Mangani D, 2023).

- Data analysis: AI-based analytics examines large volumes of data to identify patterns, clusters, and relationships, allowing the industry to shift from mere descriptive analysis to real-time predictive modeling. Machine learning enhances processes such as risk modeling, identity recognition, fraud detection, or credit underwriting.

- Report Writing: AI has made it possible to generate reports and summaries by compiling extensive structured financial data and organizing it into coherent paragraphs that highlight the key aspects of various financial transactions (Nader Al-Fard Qaboosh, 2018, pp. 25-26).

- Investment Management: AI algorithms are increasingly being utilized in investment management processes. These algorithms can make data-driven investment decisions by analyzing vast amounts of market data, news, and historical trends. AI-based systems assist in portfolio management, risk assessment, and the development of trading strategies, thereby enhancing overall investment performance (Ridzuan et al, 2024, pp. 96-97).

In China, the smart investment sector is primarily dominated by internet-based enterprises, financial information technology companies and traditional financial institutions such as fund management and securities companies. The country's first domestic smart investment platform, "Capricorn Investment," was launched by the Commercial Bank of China in 2016. Subsequently, Shanghai Pudong Development Bank introduced a similar AI-based service via a "financial intelligence" robot. Several banks, including the Industrial and Commercial Bank of China, Ping An Bank, Ever bright Bank, Guangyuan Intelligent Investment, and the Industrial and Commercial Bank of China started to adopt AI investment technologies in 2017 (Wang, D, 2017, pp. 70-72).

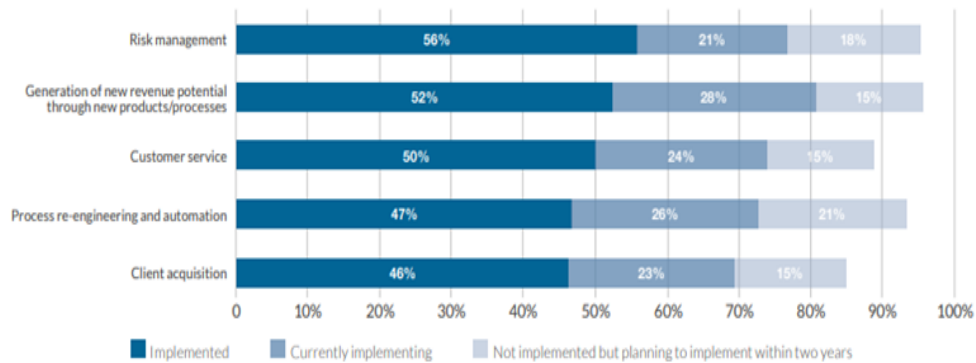
Financial technology (FinTech) companies are leading the application of artificial intelligence across all sectors, outperforming traditional companies in leveraging AI to generate new revenue streams. However, traditional companies currently exhibit higher overall rates of AI implementation (Cambridge Centre for Alternative Finance, & World Economic Forum, 2020, p. 26).

As shown in Figure (02), the adoption of artificial intelligence across a wide range of companies is categorized into three stages: already implemented, currently being implemented, and planned for implementation within two years. The data covers five main business areas:

- Generating new revenue through innovative products or processes;

- Customer acquisition;
- Risk management;
- Customer service;
- Process reengineering and automation.

Figure (02): Artificial intelligence adoption statistics across a broad sample of companies



**Source:** (Cambridge Centre for Alternative Finance, & World Economic Forum, 2020, p. 26)

Figure (02) demonstrates that risk management leads AI adoption, with 56% of companies having integrated AI models to reduce financial losses through predictive tools. This is followed by 52% of companies using AI to generate new revenue through innovative products and processes, indicating a shift toward growth-oriented applications. AI is used in customer service by 50% of companies—particularly through chat-bots and linguistic analytics—to enhance the customer experience and response efficiency. 47% have applied AI-supported automation to reengineer their internal processes, as this area combines economic feasibility (cost savings) and increased operational efficiency, which explains the high levels of planned automation adoption. Customer attraction, including demographic and behavioral data analysis, stands at 46%, with a similar rate of planned adoption, reflecting the strategic importance of expanding customer bases (Cambridge Centre for Alternative Finance, & World Economic Forum, 2020, p. 27).

### ***III. Potential Risks and Challenges of Artificial Intelligence in the Banking Sector***

The risks of artificial intelligence in the banking sector stem from the potential exploitation of technical vulnerabilities and algorithms for fraudulent activities and data theft, as well as the adoption of inaccurate models that may lead to poor financial decisions and undermine financial stability. These risks can be summarized as follows:



**III.1. Risks of Job displacement:** One of the major concerns associated with the growing use of artificial intelligence in banking is job displacement. As AI automates routine tasks, the need for human intervention decreases. While AI may generate new roles in areas such as data analysis, algorithm development, and system maintenance, many traditional banking jobs risk becoming obsolete. There is another concern that job losses could outpace the creation of new opportunities in the short to medium term (Pal, S, 2023).

In addition to concerns about job displacement, the absence of adequate and comprehensive training could lead to a significant skills gap. This scenario echoes the digital divide that previously hindered many individuals from fully benefiting from earlier technological shifts, such as the advent of the internet (Smith, K., Abbott, M., & Centonze, M, 2024).

**III.2. Security and Privacy Risks:** Artificial Intelligence's over reliance on large volumes of data poses significant security and privacy challenges. Although AI enhances security through advanced fraud detection and behavioral analysis, it also introduces new vulnerabilities, such as the risk of cyber-attacks and malicious system manipulation (Crawford, K., & Calo, R, 2016, pp. 311-313). Furthermore, the use of AI in banking raises serious concerns regarding the protection of sensitive customer information. Unauthorized access or misuse of such data can lead to severe consequences, while regulatory frameworks often lag behind technological advancements, complicating compliance for financial institutions (Schwartz, P. M., & Peifer, K. N, 2017, pp. 115-116).

**III.3. Ethical Risks and Algorithmic Bias:** The application of AI in banking raises significant ethical concerns, particularly with regard to algorithmic bias. When AI systems are trained on data containing embedded social or historical biases, they can replicate or amplify these patterns, resulting in discriminatory outcomes (Crawford, K., & Calo, R, 2016, pp. 311-313). This could lead to exacerbate discrimination based on gender, race, or other personal characteristics, potentially exposing banks to legal or regulatory consequences (Deloitte, 2024, p. 24). In areas such as loan approval, the risks associated with human bias has now shifted to algorithmic decision-making, where unintended programming or flawed data can favor one group over another without transparent justification (RiskBusiness AI report, 2022).

**III.4. Transparency Risks of AI Algorithms:** AI algorithms often present a transparency challenge, often referred to as the “black box problem”. This issue makes it difficult to understand the reasoning behind AI system's decisions, making it complicating accountability. The lack of transparency and overreliance on AI for decision-making may undermine human judgment and responsibility

(Pal, S, 2023). Ethical concerns in AI use within banking include the responsible handling of customer data, accountability for automated decisions, and transparency in algorithmic decision-making. AI systems must adhere to established ethical frameworks and guidelines to ensure ethical practices (Jain, R, 2023, p. 3).

**III.5. Technical Risks:** Technical risks in AI adoption within banking include integrating and harmonizing AI systems with existing banking systems, the need for high-quality data for AI models, and maintaining the reliability of AI systems. Additionally, the high initial costs of implementation, including infrastructure, talent acquisition, and training, pose significant barriers (Davenport, et al, 2020, p. 25).

**III.6. Model Risks:** Model risks stem from the increasing complexity of machine learning systems, which often rely on vast structured and unstructured datasets and opaque algorithms such as neural networks. These systems involve multiple hidden decision layers, making interpretation and accountability difficult. A further limitation is the shortage of qualified experts capable of evaluating model methodologies, data outputs, and potential biases (KPMG International, 2022, p. 5).

**III.7. Deep-fake Risks:** Deep-fake technology, which uses synthetic and realistic videos or audio recordings that appear convincing and realistic, poses a growing threat to the banking sector. It can be exploited to fraudulently access customer accounts successfully imitating their identity (Deloitte, 2024, p. 18).

**III.8. Regulatory and Legal Risks:** The absence of standardized regulations and legal frameworks governing AI and machine learning in banking poses significant regulatory risks. Uncertainty about future compliance requirements leaves financial institutions without clear guidance, forcing them to navigate AI model implementation independently (KPMG International, 2022, p. 6).

**III.9. Service Provider Concentration Risks:** Service provider concentration poses a significant risk when banks rely heavily on a single third-party provider for AI services. This dependence can make institutions susceptible to service interruptions from the provider affecting both service continuity and risk management. The risk is increased when many institutions depend on a limited number of providers, raising systemic concerns. Drawing on lessons from past technology integrations, banks can improve third-party risk management (Bank Policy Institute, 2024).

**III.10. Cyber Risks:** The use of artificial intelligence, including large language models (LLMs), can increase exposure to cyber risks if not implemented responsibly. As AI becomes more integrated into banking



operations, limited transparency about how these systems function may hinder the development of effective cyber-security measures. One significant concern is the violation of privacy breaches, as AI systems process large volumes of sensitive data—such as financial transactions and personal information—making them attractive targets for cyber-attacks or internal data leaks (Deloitte, 2024, p. 18).

The United States has been ranked among the most vulnerable countries to cyber-security risks. In 2018, an FBI agent responsible for investigating cyber breaches stated that every American citizen should assume their personal data (identifying information) has been compromised and stored on the Dark Web, a hidden part of the Deep Web used to facilitate criminal activities. Some estimates suggest the Deep Web is up to 5,000 times larger than the Surface Web and continues to grow at an immeasurable rate.

#### ***IV. Risk Management: AI-Powered Banks :***

AI tools are significantly enhancing the risk management of the banking sector by analyzing large volumes of data and detecting suspicious patterns in real time. This capability enables institutions to predict and prevent potential losses before they occur. Additionally, these technologies contribute to the automation of control processes and improve regulatory compliance with greater accuracy and efficiency. In this context, the following section will examine the role of artificial intelligence in mitigating operational risks in banking:

***IV.1. Operational Risk Management:*** The use of artificial intelligence in operational risk management, initially focused on preventing external losses such as credit card fraud, has since expanded to encompass areas such as document analysis, repetitive transaction processes, money laundering detection- tasks that require the analysis of large data sets (Aziz, S., & Dowling, M, 2019, pp. 33-34).

In addition to external threats, AI also addresses internal sources of operational risk, particularly human error. For example, JPMorgan Chase reported that 80% of loan servicing errors resulted from misinterpretation of contracts. In response, the bank implemented a contract intelligence platform, COIN (2016), which uses machine learning to analyze 12,000 credit agreements annually and extract relevant data within seconds—a task that would otherwise require an estimated 360,000 human work hours (Swankie, G. D., & Broby, D, 2019).

***IV.2. Model Risk Management:*** AI/ML-based algorithm results must remain interpretable to all stakeholders—customers, management, and regulators. In credit assessment, for example, it is crucial to explain the factors behind an application's rejection (e.g. salary or savings) and suggest ways to improve the customer's score. Transparency and interpretability are essential to ensure proper algorithm performance (KPMG International, 2022, p. 6).



**IV.3. Credit Risk Management:** Artificial intelligence (AI) has significantly influenced credit risk assessment in banking sector, including credit risk assessment. One of its major impacts is the improvement of predictive analytics through machine learning algorithms. AI-based models can process vast amounts of data, such as borrower profiles, transaction histories, and economic indicators, to identify patterns and evaluate creditworthiness with greater accuracy than traditional methods. This improved capability allows banks to detect potential defaults or delinquencies earlier in the lending process, thereby reducing losses and strengthening portfolio performance (Brown, M, 2024, p. 32)

**IV.4. Detecting Suspicious Financial Transactions:** AI enhances transaction security by monitoring and analyzing patterns in real time to detect anomalies that may indicate fraud or unauthorized access. Through the use of machine learning, AI systems learn typical transaction behavior and flag deviations as suspicious. For instance, if a credit card purchase occurs abroad shortly after one in the customer's home country, the system may identify it as suspicious and trigger an alert for verification before completing the transaction (Ridzuan et al, 2024).

**IV.5. Financial Fraud Prevention:** AI supports financial fraud prevention by analyzing large data sets to detect suspicious patterns and behaviors. It can identify anomalies such as unusual spending or rapid transactions from different locations. For instance, an AI-powered fraud detection system may flag ATM fraud if it detects multiple withdrawals from various machines using the same debit card in a short time. The system then alerts the customer and the bank's fraud team, and the account is automatically frozen (Ridzuan et al, 2024, p. 98)

**IV.6. Predictive Analysis for Risk Management:** AI's ability to analyze large data sets and detect patterns is critical to the banking sector. Predictive analysis enables banks to make data-driven decisions, enhance forecasting accuracy, and reduce uncertainty (Chen, Chiang, & Storey, 2012, p. 1165). In risk management, it aids in identifying potential threats and implements preventative measures. AI models can assess various factors that influence a customer's repayment ability, leading to more precise credit risk evaluations (Buchanan, 2019).

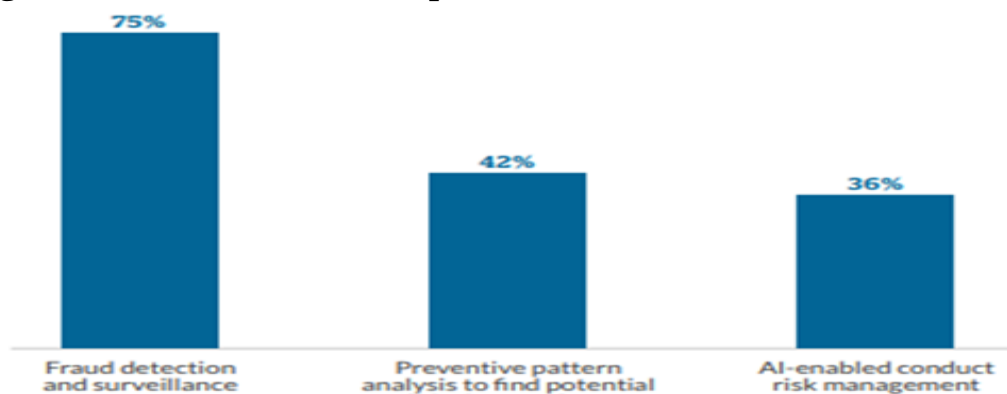
**IV.7. Cyber-security Risk Mitigation/Fraud Control:** Banking institutions increasingly use AI tools to manage risks associated with third-party technologies. AI models enhance operational efficiency and mitigate risks in cyber-security and fraud control. Machine learning tools are currently used to automate tasks such as detecting phishing attempts and improving threat awareness. As these technologies evolve, they offer opportunities for broader applications in fraud prevention, including anomaly detection and behavioral analytics (Bank Policy Institute, 2024).

**IV. 8. Regulatory Compliance:** Many banking institutions are utilizing AI tools to facilitate compliance with the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) requirements and regulatory standards set by banking supervisory bodies. These tools help detect suspicious activities, such as money laundering or sanctions violations, and expedite the processing of complex data patterns, potentially improving reporting times (Bank Policy Institute, 2024).

**IV.9. Managing Bias Risk:** To ensure fairness in AI/ML and mitigate bias, financial institutions must define their concept of "fairness" as a prerequisite for testing models. Moreover, organizations should establish a fairness verification entity within the model risk management framework, taking into consideration the need for new skills, methods, and tools (KPMG International, 2022, p. 13).

Figure 03 compares the three most important AI use cases in risk management based on current adoption rates, illustrating the percentage of companies that have already implemented these applications.

**Figure (3): The three most important use cases for AI in risk management based on current adoption rates**



Source : (Cambridge Centre for Alternative Finance, & World Economic Forum, 2020, p. 30)

From the previous figure, it is evident that fraud detection is a top priority in financial institutions' risk management, accounting for an estimated 75% of the total, due to significant losses caused by financial fraud. AI applications in this area have demonstrated immediate and measurable effectiveness, prompting nearly a third of companies to adopt them. Preventive analysis accounts for 42% of the total, requiring extensive, clean data and models capable of detecting infrequent patterns, which requires more time and effort before yielding clear investment returns. Behavioral risk management accounts for 36% of the total. Despite the regulatory importance, application of NLP and behavioral analysis, which involve processing vast amounts of textual and sensitive data, face privacy and governance challenges, slowing adoption.



## ***V. Models for Artificial Intelligence Risk Management in Banks :***

During the 1980s, global banking systems, especially the United States, witnessed a significant increase in bank failures. To address these challenges, regulatory bodies began adopting different models within their banking supervision practices, strengthening their early warning systems. Therefore, quantitative models and AI tools have now become a key complement to traditional supervision, helping bank regulators monitor the risks they face. Among the most important models of AI-based risk management are the following:

***V.1. SAS (Statistical Analysis System) Risk Management Model:*** SAS is a global leader in data analytics and artificial intelligence, serving over 70,000 client locations in 138 countries, including 93 of the Fortune Global 500. Founded in 1976 at the University of North Carolina, SAS has maintained its position as a leading private company, allocating over 20% of its annual revenue to research and development (SAS Institute Inc. (n.d.), 2025)

The term "SAS" originally referred to "Statistical Analysis System," but as the platform has evolved to include areas beyond traditional statistical analysis, "SAS" is now a brand name without a formal literal interpretation. Despite this, the historical meaning remains significant in understanding the company's roots and technical legacy. As SAS expanded into data mining, predictive analytics, and artificial intelligence, it ceased using "SAS" as an acronym and became a standalone brand focused on data governance and advanced analytics (Pennsylvania State University. (n.d.), 2025)

With the introduction of the SAS Viya platform, which supports cloud services and generative AI, SAS is now more closely associated with next-generation analytics technologies.

SAS operates seven R&D centers in the United States, the United Kingdom, China, Denmark, India, Japan, and South Korea, with 56 offices worldwide. The company is developing next-generation risk solutions based on cloud architecture and APIs using the SAS Viya 4 platform, which leverages AI, analytics, and data management. SAS has over 40 years of experience in analytics and business intelligence software, with 30 years of expertise in enterprise risk management (Research, hartis, 2023)

SAS provides a range of risk management solutions, integrating deep learning algorithms and predictive models to help financial institutions identify potential risks such as credit fraud and market volatility. These solutions include:

- Scalable technologies for detailed, timely analytics.
- Advanced risk analytics supported by quantitative analysis and research capabilities.



- Enterprise analytics and business intelligence platforms.
- Interest rate curve and credit spread analysis for financial decision-making.
- Out-of-the-box cash flow modeling for financial products and their valuations.

Key features of SAS risk management solutions include:

- Asset Liability Management (ALM).
- Liquidity Risk Management.
- Fund Transfer Pricing (FTP).
- Market and credit risk management.
- Integrated modeling for market risk, credit risk, and financial behavior.
- Multi-period balance sheet dynamics analysis for stress testing and financial simulation.
- Flexible risk aggregation and reporting for integrated analytical insights.
- Data integration and quality validation to ensure accurate modeling.
- Process automation and governance for operational efficiency and regulatory compliance.
- Integration with third-party models to enhance advanced analytics.
- Compliance with Basel III/IV, IFRS 9, CCAR, and BCBS requirements.
- Customizable solutions for commercial banks, property and life insurance, and capital markets.
- SAS Credit Risk Management enables the development of credit risk models using SAS, Python, and R, incorporating AI algorithms to estimate borrower default probabilities (SAS Institute Inc. (n.d.), 2025).
- Early Warning Systems to monitor financial and behavioral indicators in real time, enabling early corrective action.
- Fraud management and real-time detection of suspicious activities through machine learning.
- Anti-Money Laundering solutions for financial crime detection and accelerated investigations through case management systems (SAS Institute Inc. (n.d.), 2025).
- Automated fraud detection that reduces credit application processing time by 50–70% (SAS Institute Inc. (n.d.), 2025).

**V.2. FICO Falcon Fraud Manager for Financial Fraud Detection:** Launched in 1992 by Fair Isaac Corporation (FICO), Falcon Fraud Manager was the first commercial solution to use neural networks and artificial intelligence to analyze financial transactions in real-time, detecting payment card fraud before transactions are completed. The system relies on a predictive engine that continuously learns from previous transactions, integrating with electronic authorization systems to stop fraudulent activities within milliseconds, while



maintaining a low false-positive rate (<1%). Currently, it is used by 17 of the world's 20 largest card issuers, protecting more than 2.2 billion cards and reducing fraud losses by 50% to 75% for customers relying on it (FICO, 2024).

The system monitors data flows in real time, using machine learning analytics and anomaly detection techniques to identify threats as they occur, providing a competitive advantage for financial institutions in combating fraud and reducing financial and operational risks (Wang, H, 2019).

Thanks to its analytical capabilities, Falcon Fraud Manager can detect fraud across various domains, including credit and debit cards, e-commerce, checks, retail cards, identity fraud, and merchant fraud. It is also used for fraud detection strategy development and fraud case management across all banking products and channels. Key features include:

- ***Advanced Adaptive Analytics:***

- The system learns in real time from previously detected fraud cases.
- It uses strong correlation models to protect institutions from fraud schemes identified by third parties.
- Its analytics adapt to emerging threats, not relying solely on historical data.

- ***Identity Fraud Detection:***

- It detects fraud involving stolen, fake, or composite identities, as well as first-party fraud.
- The system identifies various fraud methods, whether organized or opportunistic, regardless of the product type or banking channel.

- ***Behavioral Analytics for Fraud Monitoring:***

- It analyzes large volumes of data to extract customer behavior patterns across millions of transactions.
- Custom behavioral lists are tailored to each customer, enabling the system to identify abnormal transactions based on these patterns.
- Unusual payments are flagged based on outlier patterns, helping detect suspicious activity.

2. ***Efficient Fraud Investigation Management:***

- The system improves case review efficiency and reduces processing time by distinguishing legitimate from fraudulent transactions in as little as 10 milliseconds.
- It includes advanced detection strategies with customizable configuration rules via a visual user interface.

- ***Seamless Integration with Banking Systems:***

- Falcon Fraud Manager integrates with systems such as FICO Origination Manager, reducing implementation time and enhancing analyst efficiency.
- It leverages modern technologies to streamline operations.



- ***Flexible Data Organization and Management:***
  - It facilitates rapid data coordination between internal and external systems, improving decision-making accuracy.
  - The system increases security and transparency in banking decision-making by moving beyond traditional processing models.

### ***V.3. IBM OpenPages with Watson Governance, Risk, and Compliance (GRC) Model:***

IBM OpenPages with Watson is an advanced, AI-powered, scalable Governance, Risk, and Compliance (GRC) solution that can operate on any cloud platform. Key features of the solution include (Computacenter, 2024) :

- Integration of separate risk management functions into a unified environment.
- Support for organizations in identifying, managing, monitoring, and reporting risks.
- Facilitation of effective regulatory compliance, particularly in a dynamic business environment.
- Continuous adherence to all relevant regulations.
- Enhanced transparency and accountability across the organization.
- Efficient and flexible risk management, with the ability to adapt to changing needs.
- Improvement of operational performance through strategic risk management.
- Alignment of organizational strategies for better outcomes.
- Tools for measuring, analyzing, managing, monitoring, and aggregating risks.
- Provision of necessary information to help managers improve compliance and risk processes.
- Enhanced collaboration through information sharing across different GRC teams.
- Improved visibility and understanding of risks within the organization.
- A comprehensive, integrated perspective on risks across various business units.
- A scalable platform that supports anywhere from 50 to 50,000 users.
- A unified, integrated data model ensuring consistency in information.
- A customizable, sophisticated, and user-friendly web-based interface.
- Pre-built GRC use cases to accelerate implementation.
- A task-centric user interface designed to simplify complex processes.
- An advanced calculation engine to identify and map Key Risk Indicators (KRIs).
- Built-in workflows that run automatically on schedule, on demand, or when a new object is created.
- A comprehensive audit system and integrated document management capabilities.

- **V.4. Katana Lens Model for Proactive Risk Oversight:**

J.P. Morgan Chase has invested significantly in developing innovative AI-powered risk management models, launching the Katana Lens platform in early 2024 after more than two years of intensive internal development. The company committed over \$10.6 billion to the technology and assembled a team of over 500 data scientists. Based on a centralized data architecture and advanced machine learning models, Katana Lens enables proactive risk analysis and prediction. The platform was initially piloted internally in the third quarter of 2023, before being officially launched for use by risk management teams in January–February 2024. Since its launch, Katana Lens has led to notable improvements in the speed of risk detection, the efficiency of risk teams, and the reallocation of human resources to more strategic tasks (Tulsi et al., 2024, p. 211).

Katana Lens is an AI-powered platform designed to proactively manage operational risk and compliance. It operates using a central data lake, updated daily from hundreds of sources within the bank, and runs numerous deep machine learning models to scan activities and detect anomalies. The platform has significantly improved decision-making speed and accuracy, increasing risk team productivity and substantially reducing losses (Tulsi et al., 2024, p. 211).

Key features of the Katana Lens platform include (Tulsi et al., 2024, p. 211) :

- A central data warehouse that aggregates data from more than 800 diverse sources daily, including trading positions, client account openings, sanctions checks, and more.
- Over 50 machine learning and deep learning models that analyze this data, detecting risk exposures, suspicious activity patterns, and anomalies indicative of emerging issues.
- Advanced data visualization dashboards that instantly highlight key risk indicators and their correlations, enabling management to address potential issues in real time.

Quantitative results demonstrating the effectiveness of Katana Lens include (Tulsi et al., 2024, p. 211):

- A 25% increase in risk management team productivity, handling 35% more processes, and allowing the redeployment of 150 full-time employees to direct roles without requiring additional hires.
- A 42% reduction in losses from early detection of risk events, saving more than \$500 million in the past year.
- Model predictions accurately identified 90% of emerging issues within seven days, enabling proactive resolution and reducing the severity of those issues by an average of 60%.



- Correlation analyses revealed new relationships, such as a 13% higher risk of default after using specific credit products, prompting policy adjustments.
- Integration of Katana Lens reduced incident analysis time from hours or days to seconds, enabling immediate responses to anomalies and errors.
- Early predictions and anomaly alerts resulted in a nearly 42% reduction in losses from undetected risks during the first year of implementation.
- Other benefits of Katana Lens include (Tulsi et al., 2024, p. 211):
- Enhanced regulatory compliance through continuous monitoring of over 600,000 rule changes annually.
- Improved risk management culture, with over 20,000 employees trained to use analytics in supporting balanced risk decision-making.
- Accelerated reporting cycles, reducing them from weeks to hours through automated insights.

## **VI. Conclusion:**

AI risks in the banking sector present several challenges, including cyber fraud, data corruption, and model complexities that may result in erroneous credit decisions. Despite these risks, AI plays a critical role in mitigating such threats through real-time fraud detection systems and proactive pattern analysis, thereby reducing losses and enhancing crisis response times. Deep learning models and compliance automation tools are vital in improving the reliability and efficiency of banking risk management, contributing to a safer and more stable financial environment. Based on the research findings, the following conclusions can be drawn:

### **Findings:**

The research on banking risks and risk management using AI in the banking sector highlights several key aspects that underscore the importance of managing and regulating AI applications in the industry:

- AI systems in banks process vast amounts of sensitive data, which increases the risk of security incidents such as data breaches and model manipulation attacks. Insufficient security measures can lead to privacy violations and compromised data integrity.
- The high complexity of deep learning models makes them challenging to understand and operate, limiting technical teams' ability to validate and control automated decisions. This can result in operational failures or delayed crisis responses.
- Banks utilize advanced machine learning techniques to analyze transaction patterns in real time, enabling fraud detection and prevention within milliseconds, with some platforms achieving false positive rates below 1%.

- AI algorithms analyze both historical and real-time data to predict potential defaults or liquidity fluctuations, aiding the development of preventative strategies and reducing potential losses.
- Natural Language Processing (NLP) technologies automatically review regulatory texts and banking obligations, generating accurate reports that enhance compliance speed while reducing manual effort.
- Deep learning models simulate extreme financial stress and market volatility scenarios, providing insights into the potential impact of risks and supporting the refinement of recovery plans.

### **Recommendations:**

To address the complex regulatory landscape surrounding the increasing use of AI in banking, financial institutions should adopt proactive compliance strategies to manage risks. The following recommendations are proposed:

- Continuously monitor and analyze AI regulations in collaboration with stakeholders across various countries, and develop a compliance roadmap that aligns with both current and anticipated regulatory requirements.
  - Establish a comprehensive process for assessing risks related to AI systems, classify AI applications based on their potential impact, and implement appropriate safeguards.
  - Document AI development processes, data sources, and algorithms used in decision-making, and ensure mechanisms are in place to provide transparent explanations of AI-driven decisions to stakeholders and affected individuals.

### **References :**

#### **Books**

1. Aziz, S., & Dowling, M. (2019), *AI and machine learning for risk management*, Palgrave Macmillan, Switzerland AG.
2. Majid Ahmed. (2018), *Artificial Intelligence in the United Arab Emirates*, Department of Economic Studies and Policies, Abu Dhabi, United Arab Emirates.
3. Mohammad Al-Hadi Mohammed. (2011), *Telecommunications Technology and Information Networks*, Academic Library, Cairo, Egypt.
4. Russell, S., & Norvig, P. (2020), *Artificial Intelligence: A Modern Approach* (4th ed.), Pearson.

#### **Journal Articles**

1. Chen, H., Chiang, R. H., & Storey, V. C. (2012), *Business Intelligence and Analytics: From Big Data to Big Impact*, MIS Quarterly, 36(4), 1165–1188.
2. Crawford, K., & Calo, R. (2016), *There is a blind spot in AI research*, Nature, 538(7625), 311–313.



3. Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020), *How Artificial Intelligence Will Change the Future of Marketing*, *Journal of the Academy of Marketing Science*, 48, 24–42.
4. Jain, R. (2023), *Role of artificial intelligence in banking and finance*, *J. Manag. Sci.*, 13, 1–4.
5. Nader Al-Fard Qaboosh. (2018), *Internet Banking*, *Journal of Banking*, 19(5), 25–26.
6. Nasira Bouba'aba, Shahrazad Al-Wafi & Hamza Boutghan. (2021), *The Role of Big Data and Artificial Intelligence in Combating the COVID-19 Pandemic—Successful International Experiences*, p. 131.
7. Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024), *AI in the financial sector: The line between innovation, regulation and ethical responsibility*, *Information*.

### **Seminar Articles :**

1. Buchanan, B. G. (2019), *Artificial Intelligence as Structural Estimation: Economic Interpretations of Deep Blue, Bonanza, and AlphaGo*, *Brookings Papers on Economic Activity*, Conference Draft.
2. Wang, D. (2017), *Traditional financial institutions are ready to move. Is it more advantageous to set foot in intelligent investment advisory*, pp. 70–72.

### **Internet & Reports**

1. Artificial Intelligence Index Report. (2024), *Introduction to the AI Index Report*, *Stanford Institute for Human-Centered Artificial Intelligence*, <https://www.aiindex.org/> (consulted on November 19, 2024).
2. Bank Policy Institute (BPI). (2024, April), *Navigating artificial intelligence in banking governance and risk management frameworks*, <https://www.bpi.com> (consulted on March 4, 2025).
3. Brown, M. (2024), *Influence of artificial intelligence on credit risk assessment in banking sector*, *International Journal of Modern Risk Management*, <https://www.iprjb.org/journals/index.php/IJMRM/article/view/2641> (consulted on March 5, 2025).
4. Cambridge Centre for Alternative Finance & World Economic Forum. (2020), *Transforming paradigms: A global AI in financial services survey*, [https://assets.ey.com/content/dam/ey-sites/ey-com/en\\_gl/topics/innovation/ey-why-a-i-will-redefine-the-financial-services-industry-in-two-years.pdf](https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/innovation/ey-why-a-i-will-redefine-the-financial-services-industry-in-two-years.pdf) (consulted on April 2, 2025).
5. Computacenter. (2024, May), *IBM OpenPages with Watson: GCloud 14 – Cloud Software*, <https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/92783/764719409727745-service-definition-document-2024-05-01-1200.pdf> (consulted on April 5, 2025).
6. Deloitte. (2024), *AI in banking: A transformative opportunity*, <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/financial->



- [services/deloitte-cn-fsi-ai-in-banking-en-240805.pdf](#) (consulted on January 16, 2025).
7. FICO. (2024), *Falcon® Fraud Manager innovation timeline [Infographic]*, <https://www.fico.com/en/latest-thinking/infographic/fico-falcon-fraud-manager-innovation-timeline> (consulted on April 11, 2025).
  8. KPMG International. (2022), *Modern risk management for AI models: Re-imagining the model risk management function for artificial intelligence/machine learning models*, <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/07/modern-risk-management-for-ai-models.pdf> (consulted on April 2, 2025).
  9. LinkedIn. (2025), *How SAS Supports Credit Risk Management*, <https://www.linkedin.com/pulse/how-sas-supports-credit-risk-management-1f/> (consulted on April 11, 2025).
  10. Pal, S. (2023, January), *Artificial intelligence in banking: Risk or reward?*, <https://www.researchgate.net/publication/378440228> (consulted on January 13, 2025).
  11. Pennsylvania State University. (2025), *Lesson 1.1: What is the SAS System? STAT 480: Statistics II*, Penn State World Campus, <https://online.stat.psu.edu/stat480/lesson/1/1.1> (consulted on April 26, 2025).
  - Research, hartis. (2023), *Vendor Analysis: SAS – ALM Technology Systems*, Infopro Digital Services Limited, <https://www.sas.com/content/dam/SAS/documents/analyst-reports-papers/en/chartis-alm-technology-systems-vendor-analysis-113575.pdf> (consulted on April 11, 2025).
  12. RiskBusiness AI report. (2022, November), *Artificial intelligence in banking: Risks and benefits*, <https://riskbusiness.com/wp-content/uploads/2022/11/Ai-November-Report-V2.pdf> (consulted on April 12, 2025).
  13. SAS Institute Inc. (2025), *Credit Risk Management Analytics Software*, SAS, [https://www.sas.com/en\\_us/solutions/risk-management/solution/credit-risk-management.html](https://www.sas.com/en_us/solutions/risk-management/solution/credit-risk-management.html)? (consulted on April 3, 2025).
  - Schwartz, P. M., & Peifer, K. N. (2017), *Transatlantic Data Privacy Law*, *Georgetown Law Journal*, 106, 115–179.
  14. Smith, K., Abbott, M., & Centonze, M. (2024), *The age of AI: Banking's new reality*, Accenture, <https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Age-AI-Banking-New-Reality.pdf#zoom=40> (consulted on April 4, 2025).
  15. Swankie, G. D., & Broby, D. (2019), *Examining the Impact of Artificial Intelligence on the Evaluation of Banking Risk*, [https://pure.ulster.ac.uk/ws/files/98692162/Swankie\\_Broby\\_2019\\_Examining\\_the\\_impact\\_of\\_artificial\\_intelligence\\_on\\_the\\_evaluation\\_of\\_banking\\_risk.pdf](https://pure.ulster.ac.uk/ws/files/98692162/Swankie_Broby_2019_Examining_the_impact_of_artificial_intelligence_on_the_evaluation_of_banking_risk.pdf) (consulted on March 14, 2025).



16. Tulsi, K., Dutta, A., Singh, N., & Jain, D. (2024, Jan–Feb), *Transforming Financial Services: The Impact of AI on JP Morgan Chase’s Operational Efficiency and Decision Making*, International Journal of Scientific Research & Engineering Trends, [https://ijsret.com/wp-content/uploads/2024/01/IJSRET\\_V10\\_issue1\\_138.pdf](https://ijsret.com/wp-content/uploads/2024/01/IJSRET_V10_issue1_138.pdf) (consulted on April 23, 2025).
17. Wang, H. (2019, September), *The contribution of FICO Falcon Fraud Manager to the bank industry*, Multimedia University, <https://www.researchgate.net/publication/341869377> (consulted on April 9, 2025).