Chapter 11
Artificial Intelligence and Operational Risk Management:
A Qualitative Analysis in the Moroccan Banking Sector

Hajar El Haji
https://orcid.org/0009-0006-7737-4504
Mohammed First University, Morocco

Oumayma Aitmoussa
https://orcid.org/0000-0002-3355-4742
Mohammed First University, Morocco

ABSTRACT

This paper explores the impact of artificial intelligence (AI) on operational risk management in the Moroccan banking sector through a qualitative case study conducted at Banque Populaire. The objective is to understand how AI, particularly in front-office operations, contributes to risk reduction, improved operational efficiency, and process automation. The results reveal a growing integration of AI, particularly through chatbots and automated services, helping to limit human error and reduce workload. However, challenges remain, related to both technical aspects (outages, cybersecurity, system interoperability) and human aspects (resistance to change, uneven adoption across customer segments). The study also highlights that the post-Covid context and accelerated digital transformation require banks to continually adapt their governance, information systems, and training practices. AI thus appears to be a major strategic lever for strengthening banks' operational resilience, provided it is accompanied by appropriate organizational preparation.

DOI: 10.4018/979-8-3373-1737-3.ch011

1. INTRODUCTION

Artificial intelligence (AI) represents a major advancement in the digital transformation of banks. It plays a vital role in improving operational efficiency, personalizing services, and managing risks. According to Brynjolfsson and McAfee (2017), AI reduces human intervention in repetitive processes, thus limiting operational errors and increasing productivity.

Well before the emergence of generative AI applications, financial institutions had already been relying on artificial intelligence technologies to address a variety of strategic and operational challenges.

Banks, for example, have used AI to streamline internal processes, enhance operational efficiency, and strengthen risk management frameworks. Today, the rapid democratization of AI tools—driven by technological innovation, reduced costs, and broader accessibility—is accelerating their widespread adoption across the financial sector. This momentum is also drawing increasing attention from regulatory authorities, who are examining the prudential, behavioral, ethical, and systemic implications of AI deployment within complex financial ecosystems.

Among the most widely adopted historical applications are customer service chatbots, fraud detection systems—particularly for anti-money laundering (AML) and counter-terrorist financing (CTF) purposes—as well as the automation of credit and insurance underwriting. Although these use cases are not entirely new, they have been significantly transformed and enhanced by recent technological advances, notably in data processing, machine learning algorithms, and predictive analytics.

In this context, financial institutions are making substantial investments in the development and deployment of AI-based solutions.

This investment momentum reflects strong expectations in terms of efficiency gains, cost reduction, and productivity improvements. According to McKinsey (2024), generative AI could generate between $200 billion and $340 billion in annual value creation—representing approximately 2.7% to 4.7% of the total revenue of the financial industry. For instance, banking sector spending on generative AI is projected to increase from $3.86 billion in 2023 to nearly $85 billion by 2030, with a significant portion allocated to infrastructure development and the recruitment of specialized talent in AI and data science.

However, despite the enthusiasm surrounding these innovations, institutions are adopting a relatively cautious approach when it comes to implementing generative AI in highly sensitive services or those with significant customer exposure. This cautious stance is driven by multiple factors, including regulatory uncertainty, reliance on third-party model providers, concerns about customer impact, and the need to safeguard data privacy and confidentiality.