

DIGITAL TRANSFORMATION AND OPERATIONAL RISK CONTROL WHAT IMPACT ON BANKING?

Abdel hakim HDJ ALI *

Expert, Formateur en gestion des risques, Algeria
Abdelhakim.hadjali@outlook.fr

Received : 18 /06/20 25

Accepted : 01/07/ 20 25

Published : 01/07/20 25

Abstract:

This report explores the intersection between digital transformation and operational risk management in the banking sector. It highlights how the integration of emerging technologies such as AI, big data, cloud computing, and blockchain can enhance operational efficiency and risk monitoring. However, it also emphasizes the new challenges introduced, particularly in terms of cybersecurity and technological complexity. The study examines how financial institutions must adapt their risk management frameworks to both leverage the benefits and mitigate the risks of digital transformation.

Keywords: Digital transformation, Operational risk, Cyber Security, Financial institutions.

JEL Classification Codes : O33 ; G32, K23, G21.

1. Introduction :

Digital transformation represents a radical change in the way businesses, including financial institutions, operate and interact with their customers. It refers to the integration of digital technologies into all aspects of an organization, fundamentally changing the way it operates and delivers value to its customers, affecting everything from internal processes to interactions with customers and partners.

At the same time, controlling operational risk is becoming crucial to ensuring the stability and reliability of banking services.

These two concepts may seem far apart, but in practice, is there any interaction or correlation between digital transformation and operational risk management?

Does digital transformation offer significant opportunities to improve operational risk management through automation, data analysis and more robust systems?

Can digital transformation also introduce new challenges, particularly in terms of cyber security, which financial institutions need to address with appropriate strategies to balance the benefits and risks.

We will discuss the context of the emergence of digital transformation and the adoption of advanced technologies such as artificial intelligence, big data, cloud computing, and block chain to optimize processes, leading to major changes in business and operational models.

Banks and other financial institutions, because of their critical nature and role in the economy, are particularly sensitive to operational risks, and we will also discuss how this notion of operational risk is evolving with the introduction of complex automated systems, increasing vulnerability to cyber-attacks, system failures, and technological human error.

* Corresponding Author

2. DIGITAL TRANSFORMATION-FUNDAMENTAL CONCEPTS

The term “digital transformation” is now ubiquitous. From the media to corporate boardrooms, and from experts to software vendors, many did not initially take the digital revolution seriously. Yet suddenly, many of them have become self-proclaimed evangelists of the concept without truly understanding what it entails. In short, everyone seems to welcome change... as long as it remains superficial and ultimately reverts to the status quo. Fortunately, some more visionary organizations have clearly grasped the urgency and significance of the challenge for their future or even their survival.

Far from limiting their actions to a hackathon (an innovation contest with startups), a Facebook page, or an incubator, they have developed a far more ambitious and long-term vision, supported by top management and genuine human and financial resources. AXA, AccorHotels, and SNCF, for instance, have sent a clear signal to the market by launching digital transformation programs worth several hundred million euros, involving nearly every level of their organizations (Ducrey & Vivier, 2016)

2.1. What is Digital Transformation?

Digital transformation involves integrating digital technologies into all areas of a business, fundamentally changing how it operates and delivers value to customers (Ostle, 2007).

It is far more than a mere technological shift. It represents a radical transformation in the way companies operate, interact with customers, and adapt to rapid market changes (Company, 2016).

According to Deloitte Insights (2020), digital transformation is the process of integrating digital technologies across every facet of a business, fundamentally altering how you operate and deliver value to customers.

The Organization for Economic Co-operation and Development (OECD)[†] defines digital transformation as the integration of digital technologies into all aspects of society, including the economy, businesses, public administration, and the daily lives of citizens. This transformation involves a profound reorganization of economic and social models, with the growing adoption of technologies such as artificial intelligence, the Internet of Things, big data, and digital platforms.

The OECD emphasizes that digital transformation goes beyond merely digitizing existing processes. It requires a rethinking of strategies and organizational processes to fully leverage new technologies. This includes:

- ✓ Innovation in products and services,
- ✓ Enhancement of operational efficiency,
- ✓ Strengthening stakeholder engagement through digital means.

In conclusion, digital transformation is a global and multidimensional phenomenon that is redefining traditional structures and practices while creating new opportunities for economic and social development.

2.2. Digital Disruption: Technological Change is Reshaping the World

The renowned Austrian economist Joseph Schumpeter already discussed the concept of “creative destruction” back in 1911. However, since the advent of computing and then the internet, the world, society, and businesses have experienced an acceleration of change unlike anything before. More than 4.15 billion people can now exchange information almost instantly, without geographic constraints and at a low cost—including digital services and products like music, news, videos, or e-books. Bandwidth, processing power, storage capacity, miniaturization, the number of smartphones... all technological factors are progressing almost exponentially. While each innovation is promising on its own, when combined and applied across industries, they generate a veritable tsunami of innovations that is transforming every sector at lightning speed (Ducrey & Vivier, 2016).

According to the OECD, the impact of digital transformation on economies and societies has evolved rapidly over time.

[†] The Organization for Economic Co-operation and Development

2.3. Evolution of Digital Transformation in the Banking Sector

1960s–1980s: Introduction of Computer Systems Banks began using computers to automate internal processes such as accounting and transaction processing, significantly improving efficiency and reducing errors.

1990s: The Rise of the Internet and Online Banking The advent of the internet enabled banks to offer online services, giving customers easier access to their accounts and transactions. This era marked the beginning of e-banking, transforming the way banking services were delivered.

2000s: Explosion of Mobile Banking and Digital Services With the rise of smartphones, mobile banking apps became widespread, allowing customers to carry out banking transactions from their mobile devices, making banking more accessible and convenient. Banks introduced new digital services such as SMS alerts, mobile payments, and digital wallets.

2010s: Big Data, Artificial Intelligence, and Fintech The use of big data enabled banks to analyze customer behavior and personalize offerings. Predictive analytics tools improved fraud detection and risk management.

Artificial intelligence enabled the development of chatbots for customer service, automation of back-office processes, and more sophisticated analytics for credit scoring and investment management.

Fintech companies introduced disruptive innovations in the banking sector, pushing traditional banks to innovate in order to stay competitive.

2020s: Blockchain and Open Banking Blockchain technology began to be used for secure transactions, international payments, and digital identity management.

With regulations such as PSD2 in Europe, banks were encouraged to share financial data via APIs, fostering innovation and enabling the development of new financial services.

This evolution of digital transformation over time has enabled the banking sector to achieve:

Improved Customer Experience: Faster, more personalized, and secure services, with customers able to access a wide range of financial services anytime and anywhere.

Operational Efficiency: Automation and advanced analytics have reduced operational costs and improved efficiency.

Increased Competition: The rise of fintech and large tech firms in the financial sector has intensified competition, pushing traditional banks to adopt new technologies more quickly.

Better Management of Operational Risk

Identifying Technologies to Strengthen Control and Governance Improved operational risk management requires identifying control technologies that can be integrated to enhance oversight and governance. This may include the use of fraud detection solutions, real-time monitoring systems, and data analytics technologies. ((2012), n.d.)

Digital Transformation, A Living, Evolving Matter!

Digital technology is a living and evolving entity. Its rapid pace of change challenges companies, as the time constants of technology (such as Moore's Law) differ significantly from those of organizations (which involve human factors).

However, the speed at which users and consumers adopt new digital practices is extremely fast. New digital players focus on creating experiences and uses that are accessible to the broadest audience (for example, tablets gained traction among seniors faster and more effectively than PCs). The graph below illustrates the time needed to reach 50 million households equipped with new technologies. The acceleration is staggering.

This is one of the key challenges of digital transformation : to minimize the number of companies and more broadly, individuals (though that's beyond the scope here) that fall behind, are left on the sidelines, or simply disappear. (Delorme, 2015)

3. Current Trends in Emerging Technologies for Risk Management

Digital transformation, which redefines companies' internal processes, is driven by several emerging technologies that are revolutionizing risk management. Among these, **Cloud Computing**, **Big Data**, **Blockchain**, the **Internet of Things (IoT)**, and **Artificial Intelligence (AI)** stand out for their ability to reshape not only how companies process information but also how they anticipate and manage risks. Each of these technologies brings its own set of opportunities and challenges to operational risk management.

3.1. Cloud Computing: Toward Flexible and Secure Resource Management

Cloud computing enables companies to access on-demand computing resources without investing in expensive infrastructure. This service-based model, delivered via the internet, offers unprecedented flexibility in managing operational risks.

Organizations can adjust their storage and processing capacity based on real-time needs, thereby enhancing resilience to unexpected events such as system failures or cyberattacks. Furthermore, the redundancy of data stored across multiple servers strengthens business continuity in the event of incidents.(Erl, 2013)

3.2. Big Data: Predictive Analytics for Proactive Risk Management

The use of Big Data is transforming how financial institutions anticipate and manage risks. By analyzing vast volumes of data from various sources, companies can not only identify emerging trends but also detect anomalies or weak signals that may indicate potential threats. This ability to foresee risks before they materialize supports quicker and more informed decision-making, thereby improving the robustness of risk management.(Cukier, 2013)

3.3. Blockchain: Enhanced Transparency and Security in Transactions

Blockchain introduces a new paradigm in transaction management based on transparency and security. By decentralizing processes and making every transaction verifiable by all parties involved, this technology significantly reduces the risk of fraud. Its immutable nature—where each change is logged in a shared ledger—ensures perfect traceability, making it a valuable tool for managing sensitive financial operations.

However, adoption still faces regulatory and technological hurdles, particularly regarding scalability.(Drescher, 2017)

3.4. Internet of Things (IoT): Automation and Heightened Security Risks

IoT paves the way for unprecedented process automation, allowing businesses to boost operational efficiency while collecting real-time data.

However, the interconnectedness of devices introduces new risks, especially concerning cybersecurity. The vulnerability of connected objects can be exploited to compromise critical systems.

Thus, risk management in an IoT environment requires increased monitoring and reinforced security measures to prevent intrusions.(Antonopoulo, 2014)

3.5. Artificial Intelligence (AI): A Revolution in Risk Detection

AI is increasingly being integrated into risk management processes to automate complex tasks such as fraud detection, abnormal behavior analysis, and predictive risk modeling. Through learning algorithms, AI systems can process massive data sets and identify patterns that are difficult for humans to detect.

However, integrating AI into decision-making raises ethical concerns, especially around transparency and the explain ability of algorithmic decisions.(Genovese, 2020)

4. Operational Risk

Defining risk is far more complex than it might appear. The examples below illustrate some of the most common mistakes made during risk identification exercises.

Technology is not a risk; it is a resource. Organizations use many types of technologies, and the associated risks should be defined as potential incidents or accidents resulting from malfunctions: system outages, faulty models, incorrect pricing calculations, capacity issues, software crashes, etc.

Manual processing is not a risk either; it is a cause or risk factor. It increases the likelihood of other risks, such as omissions or data entry errors. Risks arising from manual operations include fund valuation errors, misstatements in accounting books, or failure to send reports to clients.

Compliance with laws and regulations is a priority for regulated financial institutions. While it is both a requirement and a constraint, it is not, strictly speaking, a risk. Rather, it leads to **compliance risks**, which often occur inadvertently due to the sheer number and complexity of rules to follow.

That said, some breaches may be deliberate or temporary, for example, during an adjustment period to new regulatory requirements.(Chapelle, 2020)

4.1. So, What Is Risk?

Risk is the possibility that the future outcome of a decision may differ from current expectations. It is measured in terms of variance or standard deviation of possible outcomes.(Michel Crouhy, Dan Galai, 2000)

Risk is the measure of uncertainty regarding the future that can affect a company's ability to achieve its objectives. It may result in losses or opportunities.(Jorion, 2001)

Risk represents exposure to potential financial losses due to uncertainties about future events.(Lapointe, 2010)

Risk is a situation in which future events cannot be predicted with certainty, but probabilities of different outcomes can be estimated.(Donaldson, 2005)

4.2. Operational Risk

Operational risk is defined as the risk of losses resulting from an organization's inability to conduct its operations effectively due to failures in its internal processes, systems, or because of external factors. This type of risk is associated with the day-to-day management of activities.(Timsit, 2010)

Operational risk refers to the risk of loss resulting from the inadequacy or failure of internal processes, people, and systems, or from the occurrence of external events. It includes, in particular, human errors, system failures, and fraud. (Lemoine, 2006)

The concept of operational risk is therefore extremely broad: it encompasses all risks that can cause damage, loss, or cost, either created or suffered during the company's routine operations—meaning in its daily operating cycles: infrastructure, energy, telecommunications, production, distribution, supply chains, logistics processes, document management, day-to-day operating activities and pursuit of its corporate purpose, directly or indirectly, etc.

In summary, operational risks represent all direct or indirect impacts generated by the company in its daily activities and operating cycle. Within the risk hierarchy, they follow directly after financial risks, stemming from the company's "operational core."

Their analysis will be carried out by major process families, with three specific types of operational risks being particularly important and thus treated separately : legal risks, IT risks, and social and psychosocial risks (more simply referred to as "human resources risks").(DUFOUR, 2014)

4.3. Operational Risk in Banking

With regard to operational risk in the financial sector, particularly banking and insurance, their risk management frameworks—stemming from Basel II (decree of February 20, 2007) and the upcoming Solvency II regulations—define operational risks as “the risk of losses resulting from

inadequate or failed internal processes, people and systems, or from external events, including low-frequency but high-impact events.”

Although this definition is comprehensive and highlights the extent of impacts linked to operational risks, it is often difficult for companies to apply it effectively. It also assumes a certain level of risk culture and expertise, since it is easy to confuse the concept of risk with related notions such as threats, incidents, or feared events. These difficulties complicate the collection of loss data and the development of a risk mapping.(BERNARD, 2019)

More intelligibly, operational risks include all risks that may disrupt the organization due to their potential for disorganization. These risks can include legal risks (lawsuits due to non-compliance), social risks (strikes, riots), psychosocial risks (employee suicide), or IT risks (server or system failure that paralyzes operations). For instance, according to Mr. Ferrary, “human risk is one of the components of operational risk that must be identified and managed. HRM tools and practices serve as analytical methods and means of covering this risk.” (Ferrary, 2009)

In reality, although many risks originate from operational risks, they are often underestimated in practice—even in the banking and insurance sectors where there is a regulatory requirement for provisioning them. For example, the occurrence of a market risk after exceeding certain limits—despite procedures explicitly prohibiting such breaches—constitutes a primary source of operational risk.

In practice, more attention is often paid to other types of risk such as credit risk, interest rate risk, counterparty risk, market risk, etc. These are sometimes referred to as “boundary risks” because operational risks are sometimes associated with other risks : market risk, counterparty (or credit) risk, underwriting risk, and strategic risk in particular. (Chelly, 2012)

Following media coverage of several scandals (Société Générale, AIG, UBS, JP Morgan Chase...), taking operational risk into account—even in trading rooms—has become crucial to preserve the reputation of banks and insurance companies. As Eric Lamarque points out, “If international regulatory authorities have taken up the issue, it is because the financial cost has become increasingly significant and capable of significantly affecting institutions’ profitability and capital.” (LAMARQUE, 2009)

Numerous internal reports from banking institutions and the 2010 guidelines issued by CEBS (Committee of European Banking Supervision) have highlighted operational risks related to the complexity of new financial products, which can lead to losses with systemic consequences. Another example is internal fraud, as illustrated by rogue trading cases within banks, corruption, or identity theft. These operational risks lie at the intersection of legal, economic, ethical, and compliance domains.

This perspective requires nuance. The wide range of operational risk occurrences is also highlighted by shared databases such as the **Operational Risk data exchange Association (ORX)**‡ the largest association for operational risk management in the financial services sector, created in 2002 by financial institutions seeking to share loss data.(Hübner, 2010)

This database is shared by more than 65 banks in 18 countries, including ABN AMRO, Barclays, BNP Paribas, Commerzbank, Credit Suisse, Crédit Agricole, JP Morgan, Morgan Stanley, Société Générale, Wells Fargo & Co., etc.

Between 2006 and 2010, data from this database showed that, across all operational losses by banking business lines, trading activities ranked first in terms of operational loss amount per €100 of revenue generated by business line.

Operational risk associated with trading rooms ranked second, just behind corporate finance, when the average operational loss per activity was considered. (DUFOUR, 2014)

Operational Risk data eXchange Association (ORX) is the largest operational risk management association in the financial services industry. Founded in 2002 by financial firms seeking to share loss data.

4.4. RISK MANAGEMENT IN THE DIGITAL TRANSFORMATION ERA

In the era of digital transformation, financial institutions are at the heart of a technological revolution that is profoundly reshaping their operations and risk management practices. Internal control, a fundamental pillar for ensuring process reliability and regulatory compliance, is particularly impacted by this transformation. While digital technologies bring undeniable benefits in terms of efficiency and innovation, they also introduce new challenges that require a reassessment and adaptation of existing control mechanisms. The rise of emerging technologies such as artificial intelligence (AI), blockchain, and advanced data analytics is forcing organizations to rethink their control systems to remain effective and relevant in a constantly evolving digital environment.

This section explores the implications of digital transformation on internal control within financial institutions. We begin by examining the evolution of internal control in the context of digital transformation, highlighting how control practices have adapted to technological changes. Next, we analyze emerging technologies and their impact on internal control, exploring how AI, blockchain, and process automation affect control practices.

We then address the challenges and opportunities associated with digitalization, identifying the main difficulties encountered as well as the potential benefits for internal control systems. The integration of digital risk monitoring and management tools will also be discussed, examining how digital tools can be used to strengthen control practices. Finally, we will consider change management and the training needed to effectively implement digital internal control systems.

4.5. EVOLUTION OF RISK MANAGEMENT IN A DIGITAL TRANSFORMATION CONTEXT

The financial services sector is undergoing massive transformation, and risk management runs the risk of falling behind and focusing solely on downside risks. Risk management must have a seat at the table and, to be credible, must be an integral part of the broader discussion on digital transformation—from strategy to implementation. Being a passive observer is not an option.

The scale of change is significant. One risk management leader states: "We're thinking about how to adapt to the future—how to digitize our processes and products, remove retail branches, etc. The change has significant cultural implications. We need to rethink how the bank operates." From this broader perspective, another executive adds: "We need to look at it from the perspective of the entire digitization journey."

Until now, risk management groups in banks have often played a relatively passive role in technological transformation. Generally, risk contributes only moderately to the company's IT and digital strategy, and alignment between that strategy and operational risk management planning is limited (see figure 1).

Leading banks have fostered greater engagement; their risk management groups contribute significantly to IT and digital strategy (20% of banks) and have aligned their plans with the risks associated with the IT and digital strategy (17%). According to an executive whose bank has adopted a more integrated approach, "Risk is deeply involved with our risk engine in digital transformation processes. Many processes are multi-channel with more automated decisions. We are at the heart of this process because the decision engine is now integrated with risk management." Such involvement requires a cultural shift, as another executive notes: "The front office thinks it can do whatever it wants, or use whichever platform it wants. If something fails, it's risk and finance who are left to deal with it." (Ey.com/banking risk, 2018)

Risk can help contextualize digital transformation; after all, regulations and other issues have not disappeared. One Chief Risk Officer summarizes it as follows: "The interconnection between digitization and the regulatory landscape is important. The role of risk management must evolve to be proactive and work closely with finance to guide the business and raise awareness about these connections." (Zerbib, 2019)

4.6. IMPACT OF AI AND AUTOMATION ON INTERNAL CONTROLS

Automation enables repetitive tasks to be executed with increased accuracy and reduces human error. AI, especially predictive analytics tools, allows proactive monitoring by identifying anomalies and trends before they become major issues.

Predictive Risk Analysis

Predictive Models: AI enables the creation of predictive models that anticipate future risks by analyzing large volumes of historical data and identifying trends or anomalies. These models improve institutions' ability to prevent incidents before they occur.

Scenario Simulations: With AI, institutions can run simulations of complex risk scenarios, helping them better understand the potential consequences of various events and prepare appropriate responses.

Automated Monitoring: AI facilitates real-time anomaly detection in financial transactions, such as unusual behaviors or deviations from established norms. This reduces the risk of fraud and operational errors.

Learning Algorithms: AI systems use machine learning algorithms to continuously improve their ability to identify anomalies, refining their models based on new data.

Consequences of Process Automation in Controls

Reduction of Human Errors: Automating internal control processes decreases reliance on manual interventions, reducing human error risks and improving the accuracy of controls.

Real-Time Processes: Automation also enables real-time controls, speeding up the detection and resolution of issues, thereby strengthening operational resilience. (Ey.com/banking risk, 2018)

4.7. INTEGRATING BLOCKCHAIN INTO CONTROL SYSTEMS

Blockchain offers a decentralized and immutable ledger of transactions, enhancing traceability and reducing the risk of fraud. It can be used to strengthen internal controls by ensuring data integrity and facilitating audits through a reliable source of truth.

Traceability and Transparency

Immutable Ledgers: Blockchain creates immutable and decentralized records of all transactions, offering full transparency and easy traceability. This significantly reduces data manipulation risks and improves information integrity.

Facilitated Audits: The transparency provided by blockchain simplifies both internal and external audit processes, making it easier to verify transaction compliance with applicable standards and regulations.

Fraud Reduction

Inherent Security: The decentralized and secure nature of blockchain reduces the risk of fraud, as any attempt to alter data requires consensus across the entire network, which is extremely difficult to achieve without detection.

Smart Contracting: Blockchain-based smart contracts automate the execution of agreements when a predefined set of conditions is met, thus reducing the risk of non-compliance or contract fraud.

Integration Challenges

System Compatibility: A major challenge of integrating blockchain is its compatibility with existing systems. Institutions often need to overhaul their infrastructure to effectively incorporate this technology.

Management of New Risks: While blockchain enhances security, it also introduces new risks, such as those related to cryptographic key management or dependency on specific technology platforms. (EY, 2020)

4.8. OPPORTUNITIES OF DIGITALIZATION FOR CONTROL SYSTEMS

Digitalization can positively transform control systems by enhancing their efficiency, accuracy, and adaptability. In *"Digital Transformation: Survive and Thrive in an Era of Mass Extinction"*,

Thomas Siebel provides valuable insights into how digital technologies can be integrated to optimize control processes in a rapidly changing environment and how digitalization is transforming organizational practices, including control systems.

Automation and Efficiency: Digitalization allows control processes to be automated, greatly reducing the need for human intervention and minimizing human errors. Siebel emphasizes that technologies such as business process management software and real-time monitoring tools can improve internal control efficiency. Automation makes systems faster and more accurate, enhancing organizations' ability to proactively monitor and manage risks.

Predictive Analysis and Anomaly Detection: The use of AI and predictive analytics strengthens control capabilities. Advanced data analytics tools can identify trends and anomalies before they become major problems. AI algorithms can process massive data volumes to detect unusual patterns and alert risk managers in real time, enabling quick and informed responses.

Improved Transparency and Accountability: Digitalization enhances operational transparency through advanced reporting tools and interactive dashboards. These tools offer increased visibility over control processes and make it easier to communicate control results to stakeholders. Increased transparency reinforces team accountability and improves corporate governance.

Process Agility and Flexibility: Digitalization makes control processes more flexible and adaptable. Organizations can quickly adjust their control procedures in response to regulatory or operational changes. This agility allows companies to more easily adapt to new requirements and remain competitive.

Cost Reduction: By automating processes and using advanced analytics tools, organizations can reduce the costs associated with internal controls. Digitalization decreases the need for human resources for repetitive and manual tasks, allowing resources to be reallocated to higher-value activities. (Siebel, 2019)

4.9. Challenges of Digitalization for Control Systems

In *“Digital Transformation: A Roadmap for Billion-Dollar Organizations”*, George Westerman, Didier Bonnet, and Andrew McAfee explore the complex challenges related to the digitalization of control systems. These challenges show how digitalization can complicate the management of such systems.

System Complexity and Integration: Digitalization increases the complexity of IT systems. Organizations must integrate new technologies with existing systems, which can be difficult and costly. The added complexity can also make control management more challenging, making it hard to coordinate and monitor processes across disparate systems.

Security and Privacy Risks: Digitalization exposes organizations to increased risks related to data security and privacy. Technologies such as cloud computing, the Internet of Things (IoT), and big data introduce potential vulnerabilities that attackers can exploit. Protecting data becomes a major challenge, requiring stronger controls and constant vigilance.

Change Management Challenges: Implementing new technologies and processes often requires significant adjustments in organizational structures and management practices. Resistance to change and difficulties in adapting can hinder the effectiveness of newly implemented control solutions.

Data Quality and Information Reliability: Data quality is critical for effective control systems. Digitalization involves processing large volumes of data, and poor data quality can lead to errors in controls and reporting. Ensuring the reliability of information becomes a challenge, requiring rigorous data validation and verification processes.

Regulatory Compliance and Standards: Organizations must navigate a complex and rapidly evolving regulatory environment driven by digitalization. Compliance with local and international regulations becomes more difficult to manage, and organizations must implement control systems that can adapt to constantly changing regulatory requirements.

Implementation Costs and ROI[§] : Another significant challenge is the high cost of implementing digital technologies and the often-uncertain return on investment (ROI). The investments required to modernize control systems can be substantial, and organizations must carefully assess the expected benefits relative to the costs involved.(George Westerman, Didier Bonnet, 2021)

4.10. Training and Awareness to Support Digital Risk Management

While technology can enhance risk management performance and efficiency, human talent remains essential in risk strategy and decision-making.

In *“Leading Digital Transformation: How to Reinvent Your Organization for the Digital Age”*, George Westerman, Didier Bonnet, and Andrew McAfee discuss the importance of training and awareness in the context of digital transformation.

Importance of Continuous Training: Digital transformation requires continuous training for employees at all levels of the organization. Digitalization involves adopting new technologies and new ways of working, which demand specific skills. Ongoing training helps employees acquire these skills and stay up to date with technological changes, ensuring the organization can fully leverage the benefits of digital tools.

Developing Digital Leadership Skills: It is crucial for leaders to develop digital leadership capabilities. Leaders must not only understand digital technologies but also be able to lead the cultural and organizational change required for successful digital transformation. Leadership training is key to guiding teams through the challenges and opportunities of digitalization.

Fostering a Culture of Change Awareness: It's important to build a culture that embraces change within the organization. Awareness goes beyond technical training—it also involves helping employees understand the benefits of digital transformation and how these changes will improve operations and outcomes. A positive change culture helps overcome resistance and encourages employee engagement.

Effective Communication Strategies: Clear and transparent communication strategies are recommended to support digital transformation. Effective communication helps clarify transformation goals, explain the benefits to employees, and address concerns. Regular and open communication is essential to maintain alignment and employee support throughout the transformation process.

Use of Digital Tools and Resources for Training: Using digital tools to facilitate training and skills development is a valuable option. E-learning platforms, interactive simulations, and online resources can offer flexible training opportunities tailored to individual needs. Integrating these tools into training programs allows organizations to reach a broader audience and address diverse skill requirements.

Evaluating and Adjusting Training Programs: It is critical to continuously evaluate training programs to ensure they meet employee needs and organizational goals. Organizations should monitor training effectiveness, collect feedback, and adjust programs based on results and evolving technological demands.(George Westerman, Didier Bonnet, 2014)

4.11. Digital Transformation: Opportunity or Threat for Operational Risk Control?

On the ground, what do studies and statistics say about a possible correlation between Digital Transformation and Operational Risk in the banking sector? Let's explore data from the European Central Bank and a study from ORX to try to answer the question: opportunity or threat?

Digital Transformation and Operational Risk Reduction

Digital transformation in banks is directly linked to a reduction in operational risks, especially those related to human error, which represent a significant portion of such risks.

[§] Return On Investment

Process Automation: The decline in physical bank branches is partly due to the automation of many banking processes. For instance, transactions that once required human interaction (e.g., check processing, account openings, financial advice) are now carried out via digital platforms, reducing human errors and associated risks.

Workforce Reduction: Branch closures result in a reduced workforce. While this may seem negative from a social perspective, it presents an opportunity to reduce operational risk. Fewer employees potentially mean fewer failure points related to human error, internal fraud, or non-compliant behavior.

Opportunities for Risk Management: Digital transformation allows banks to adopt more sophisticated risk management solutions, such as real-time data analytics, AI-powered fraud detection, and automated incident management. These technologies can detect and prevent risks more effectively than traditional methods.

Remaining Challenges: Despite its many advantages, digitalization also introduces new types of operational risks—particularly cyber risks. These will be addressed through the following study published by ORX via *Banking Risk and Regulation* [*Banking Risk and Regulation*, a Financial Times Specialist service, is a dedicated resource for risk owners and senior professionals in risk and compliance across the three lines of defense.]

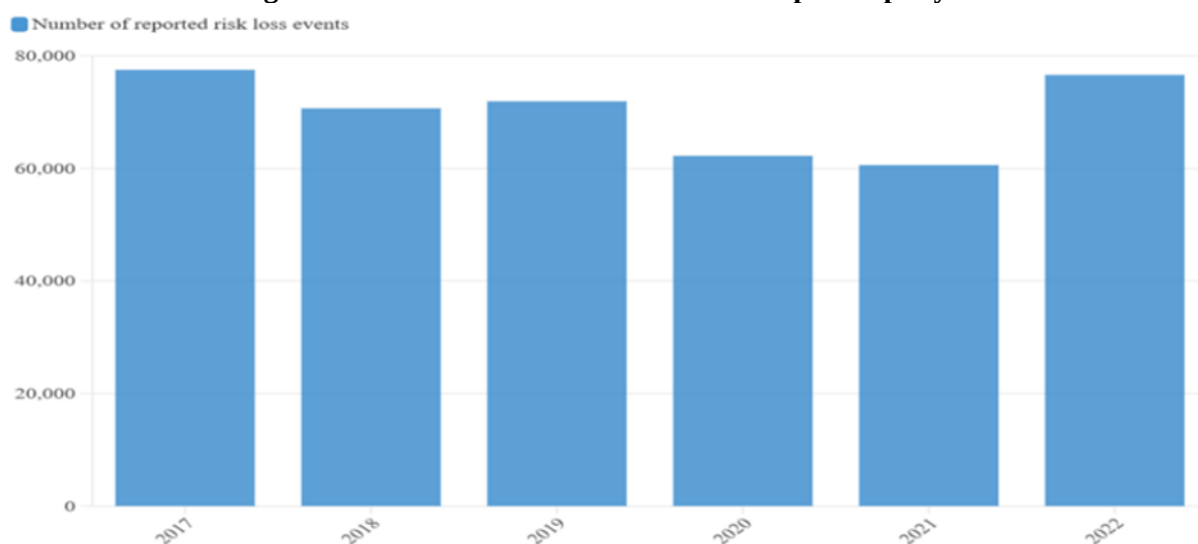
“Incidents of Operational Risk Rise by 26% Due to AI and Low-Impact Fraud”

By Giada Zampano, August 15, 2023

Generative AI has contributed to the highest number of operational risk “incidents” since 2017, according to ORX.

Data from the world’s largest operational risk association revealed that more sophisticated technology and low-impact fraud led to a reported 76,620 loss events in 2022—an increase of 26.4% (16,020 events) compared to the previous year.

Figure 1: Total number of risk loss events reported per year



Source: ORX Annual Banking Loss Report

Good news for banks: it appears that the sector continues to address the overall number of risk-related losses. However, ORX is concerned that AI and other emerging technologies may contribute to an increase in incidents linked to criminal activity.

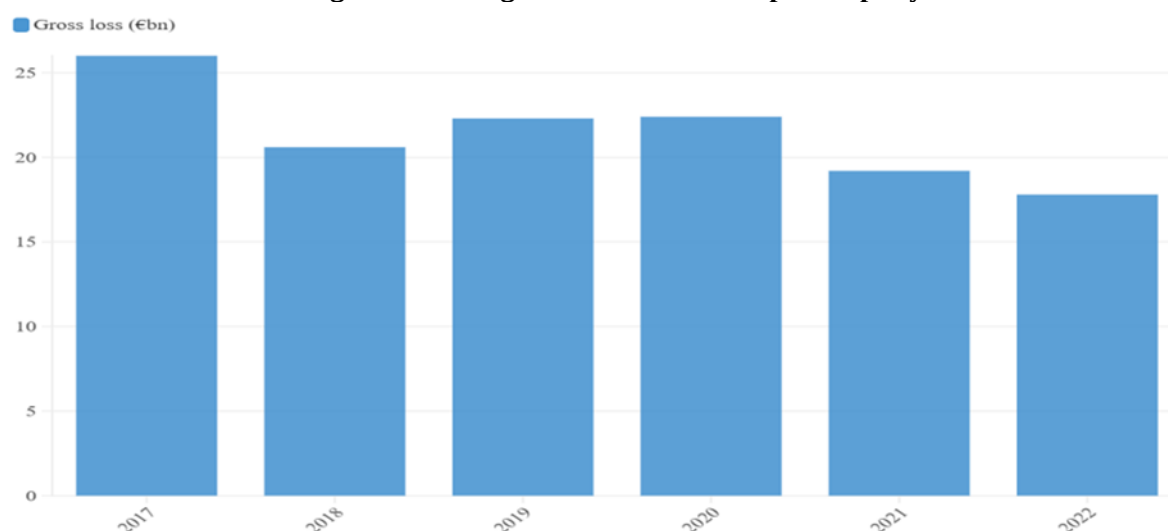
“Our members are particularly concerned that generative AI models, such as large language models, could be used to produce targeted scams specifically tailored using personal data, often harvested from social media,” says Steve Bishop, Director of Research and Information at ORX.

Lowest level of gross operational risk losses in 2022

Global figures on annual operational risk losses published by ORX show that, although 2022 was a year of geopolitical and economic turmoil as well as a period of significant digitalization, banks recorded the lowest levels of gross operational risk losses seen in recent years.

The 76,000 operational risk incidents amounted to a total of €17.8 billion in gross losses. This represents an average decrease of €1.6 billion per year, and a drop of €8.2 billion in total gross losses between 2017 and 2022, according to ORX.

Figure 2: Total gross loss of events reported per year



Source: ORX Annual Banking Loss Report

The annual report on banking losses also revealed that:

- ✓ Eight out of ten incidents (80%) occurred in banks' retail and commercial activities.
- ✓ Around one in twenty people (6%) worked in the trading and investment sector.
- ✓ About one in ten cases (10%) occurred in banks' corporate activities.

For the years 2017 to 2022 :

- ✓ Retail and commercial banking lines of business accounted for the largest share of total gross losses (61%).
- ✓ Trading and investment activities incurred 19% of the losses.
- ✓ Corporate functions represented 16%, with the remaining 4% attributed to other business areas.

Increase in frequency also linked to low-value fraud

ORX notes that the increase in the number of reported events is also linked to a widespread rise in external fraud cases. Since this rise is not reflected in gross losses, the increase in frequency can be attributed to a surge in low-value fraud incidents.

The highest frequency for most business lines is due to events classified under the category "Execution, Delivery & Process Management" – losses resulting from failed transaction processing or failures in managing processes and relationships with business counterparties and vendors – with a total of 108,486 events.

Some 38% of firms experienced in 2022 the highest number of external fraud events ever recorded. North American retail banks were the most affected, with events in this category nearly doubling in 2022 compared to 2021.

Fraudsters may exploit generative AI

"It will be interesting to see whether the increased use of generative AI and other similar emerging technologies will further raise the figures next year, as we're seeing this become more widespread with potential for misuse," says Bishop.

In an interview with *Banking Risk & Regulation*, he explained that the risks still revolve around traditional social engineering techniques, impersonating individuals or companies, and using facts to make things seem legitimate.

With AI, fraudsters may be able to do this on a much larger scale. On the other hand, AI could also be used as a tool for fraud prevention. “This is an area where machine learning models have long been used to detect suspicious activity patterns, and as techniques evolve, financial institutions must stay on top of developments to ensure they protect their customers effectively,” he notes. Bishop indicates that early indications for 2023 suggest that the frequency of fraud-related losses remains high. But many banks are also “actively evaluating and continuously improving their control frameworks, or safeguards, in light of rapidly evolving AI and broader technological developments.” (Zampano, 2023)

5. CONCLUSION

It therefore seems legitimate to question the existence of a correlation between digital transformation and operational risk control — at least from a theoretical standpoint.

On the one hand, the answer tends to be affirmative.

Indeed, digital transformation, by reducing the number of physical branches and automating a wide range of processes, offers banks a powerful lever to improve operational risk management. Reducing human error and adopting advanced technologies enables banking institutions to address risks proactively and efficiently. Solutions such as real-time data analytics and automated incident management provide greater sophistication in detecting and preventing risks, turning this challenge into a strategic opportunity. This evolution not only helps optimize costs but also strengthens banks’ resilience in increasingly complex environments.

On the other hand, digital transformation is not without its challenges.

While technologies such as generative artificial intelligence (generative AI) open new avenues for strengthening fraud detection, they are also a double-edged sword. As shown in recent studies — such as that of the ORX association mentioned above — fraudsters are also leveraging these technologies to develop more targeted and harder-to-detect attacks. At the same time, the growing cyber risk has become a major issue. Process automation and system interconnectivity make institutions more vulnerable to cyberattacks, which can cause major business disruptions, theft of sensitive data, or damage to the institution's reputation.

Furthermore, banking regulators must keep pace with technological innovations, creating increasing pressure to adapt regulatory frameworks. Regulatory risk management thus becomes a major challenge. Banks must not only comply with new regulations regarding cybersecurity, data protection, and risk management but also anticipate penalties in case of non-compliance. These requirements, combined with the rapid pace of technological change, complicate risk control — particularly in an environment where advanced technologies can be both a solution and a source of vulnerabilities.

Thus, despite undeniable benefits, the adoption of these technologies requires continuous adaptation of risk management frameworks and regulations to address emerging vulnerabilities. This delicate balance between technological innovation, cyber risk management, and regulatory compliance will be explored in the practical part of this thesis. We will analyze in more detail the correlation between digital transformation and operational risk control on the ground.

6. Bibliography list:

Books

- Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media.
- Bernard, N. D. F. (2019). *Piloter la gestion des risques et le contrôle interne*. MAXIMA.
- Chapelle, A. (2020). *Gestion des risques opérationnels*. Pearson.

- Delorme, P. (2015). *La transformation digitale*. DUNOD. <https://doi.org/10.3917/dunod.delor.2015.01>
- Donaldson, J.-P. D., & J. B. (2005). *Risque et incertitude en entreprise*. Economica.
- Drescher, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps*.
- Ducrey, V., & Vivier, E. (2016). *Le guide de la transformation digitale*. EYROLLES.
- Dufour, J. D., & N. (2014). *Le coût du risque*. Gereso.
- Erl, T. (2013). *Concepts, technology & architecture*.
- George Westerman, Bonnet, D., & McAfee, A. (2014). *Digital transformation: A roadmap for billion-dollar organizations*. MIT Press.
- George Westerman, Bonnet, D., & McAfee, A. (2021). *Leading digital transformation: How to reinvent your organization for the digital age*. Harvard Business Review Press.
- Jorion, P. (2001). *Introduction à la gestion des risques*. DUNOD.
- Lapointe, F.-C. (2010). *Les risques financiers et leur gestion*. Vuibert.
- Lemoine, P. (2006). *Gestion des risques opérationnels*. Eyrolles.
- Michel Crouhy, Galai, D., & Mark, R. (2000). *Gestion des risques financiers*. McGraw-Hill.
- Siebel, T. (2019). *Digital transformation: Survive and thrive in an era of mass extinction*. RosettaBooks.
- Timsit, D. (2010). *Gestion des risques opérationnels: Théorie et pratique*. Economica.

Journal Articles

- Zerbib, O. D. (2019). The effect of pro-environmental preferences on bond prices: Evidence from green bonds. *Journal of Banking & Finance*, 98, 39–60.
- Chelly, D. (2012). Risques frontières: une bonne raison de ne pas sous-estimer les risques opérationnels. *Risques*, 2(89), 19–28.
- Cukier, K., & Mayer-Schönberger, V. (2013). Big data: A revolution that will transform how we live, work, and think. *Choice Reviews Online*, 50(12), 50-6804–50-6804.
- Ferrary, M. (2009). Les ressources humaines à risque dans le secteur bancaire. Une application de la gestion des risques opérationnels. *Gestion 2000, Mars-Avril*, 2, 85–104.
- Genovese, S. (2020). Artificial intelligence: A guide for thinking humans. *Ordo*, 71(1), 444–449. <https://doi.org/10.1515/ordo-2021-0028>
- Hübner, R. (2010). Operational risk management: Using data more effectively. *Journal of Securities Operations & Custody*, 3(4), 280–287.
- Lamarque, E. (2009). La banque sait-elle encore gérer le risque? *Revue Française de Gestion*, 193–207.

Theses/Academic Reports

- (None explicitly mentioned as theses in this batch. Let me know if any are dissertations or need to be categorized as such.)

Conference Papers / Presentations

- (None clearly labeled as conference proceedings here. Let me know if any entries like BERNARD (2019) were presented at conferences.)

Websites & Reports

- EY (2020). *Digital transformation and risk management*. Wiley.
- EY.com. (2018). *Accelerating digital transformation: Four imperatives for risk management*. <https://www.ey.com/bankingrisk>
- Zampano, G. (2023). Operational risk ‘incidents’ surge 26% because of AI and low-risk fraud. *Banking Risk and Regulation*.