MTÜ International Research, Education and Training Center

VOLUME 07 ISSUE 03 2026

SUPPORTING SUSTAINABLE BUSINESS DEVELOPMENT

Monograph

MTÜ International Research, Education and Training Center

VOLUME 07 ISSUE 03 2026

SUPPORTING SUSTAINABLE BUSINESS DEVELOPMENT

Monograph

Tallinn - 2026

JEL Codes: G30, G32, M10, M20, M21, M40, D18, E10.
UDC: 330, 334, 336, 338

Reviewers:
Isazade Namig-PhD in Business Administration, UNEC scientist, IRETC MTÜ, Shareholder, Tallinn, Estonia.
Nataliia Sheludko-Sciences Institute of Demography and Quality of Life Problems of the National Academy of Sciences of Ukraine
Skryl Vitaliia- PhD in Economics, Associate Professor. National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine.
Vitaliy Serzhanov- Doctor of Economics, associate professor, Head of the scientific grant activities department State University “Uzhhorod National University”, Ukraine.

Author's team:
Alla Dmytrenko-Doctor of Economics, Associate Professor, Professor of the Department of Finance, Banking and Taxation, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine.
Isazade Namig-PhD in Business Administration, UNEC scientist, IRETC MTÜ, Shareholder, Tallinn, Estonia.
Liana Ptashchenko-Doctor of Economics, professor, National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine.
Oksana Vovchenko-PhD in Economics, Associate Professor, Associate Professor of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine.
Vladyslav Mazurenko-Postgraduate, National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine.

The monograph examines the issues of implementing innovative digital technologies in businesses that develop according to the principles of sustainable development and compliance, as well as in companies in such important sectors of the national economy of Ukraine as the oil and gas industry and banking services. Businesses that develop on the principles of sustainable development (ESG) and compliance imperatives ensure their competitiveness, positively affecting the environment and society. At the same time, the idea is that the effective implementation of ESG and compliance should be assisted by business analytics and big data systems that allow for improved analysis of the company's financial indicators and balance sheet, allow for the creation of multidimensional profit and loss reports, and also help understand cash flow, determine the most relevant financial indicators, assess potential, and make management decisions to improve the company's performance. An example of modeling the net present value (NPV) of drilling programs is given, which showed that reducing the WACC from 20% to 15% increases the NPV of a 12-year program by 36% - more than a 15% reduction in initial capital costs. For the first time in OGI conditions in Ukraine, a dual-chain learning model was built, which simultaneously describes the learning curve of horizontal drilling (Ld) and HF (Lh). The inclusion of a multiplicative productivity function allows us to quantitatively assess the synergistic effect. The emphasis is on the fact that digitalization opens up significant opportunities for banks to optimize internal processes. The use of big data and artificial intelligence helps analyze customer behavior, predict risks and develop products that best meet consumer needs. Blockchain technologies provide transparency in financial transactions and protection against fraud. By combining advanced technologies such as blockchain and artificial intelligence with a value-based risk culture and a proactive approach to ESG and regulatory compliance, banks can successfully adapt to the challenges of the digital age.This comprehensive approach serves as a model for implementing resilient, secure, and transparent digital ecosystems that can withstand macroeconomic challenges and meet the growing needs of society.

Online edition: ISBN: 978-9908-9777-9-9 (Tallinn, Estonia)
Printed work: ISBN: 978-9908-9777-8-2 (Tallinn, Estonia)

TABLE OF CONTENTS

RISK CULTURE AS A DRIVER OF A BANK'S DIGITAL DNA

Oksana Vovchenko
PhD in Economics, Associate Professor, Associate Professor of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine, e-mail: o.s.vovchenko@gmail.com
ORCID: 0000-0001-8065-0529

Introduction

The Ukrainian banking sector is undergoing a period of intensive transformation, becoming a key driver of the digitalisation of the national economy. Thanks to the joint efforts of the National Bank of Ukraine and the Ministry of Digital Transformation, financial services are becoming more accessible, convenient and transparent for citizens. This transformation is an integral part of the digital state development strategy, aimed at integrating modern technologies into all spheres of public life.

According to the National Bank of Ukraine, there has been a steady increase in cashless payments, indicating the active adoption of digital technologies in the financial sector. Furthermore, current trends towards significantly increased data accessibility and granularity, alongside the emergence of new infrastructure and technologies such as cloud computing, APIs, DLT, Big Data, AI and others, will enable Suptech and Regtech to automate and optimise supervisory and regulatory processes [1]. The use of Suptech and Regtech tools helps to improve analytical capabilities, monitor risks in real time, make more accurate forecasts and formulate well-founded supervisory policies for both regulators and financial institutions.

The Ministry of Digital Transformation, in turn, is actively working to create a favourable environment for the development of digital financial services, in particular through the Diia project [2].

For banks, digitalisation opens up significant opportunities to optimise internal processes. The use of big data and artificial intelligence helps analyse customer behaviour, forecast risks and develop products that best meet consumer needs. Blockchain technologies ensure the transparency of financial transactions and protection against fraud.

However, in their quest for market leadership, financial services firms continue to focus on becoming fully digital; yet, according to [3], the financial industry as a whole has not fully explored what it means to be digital "from the inside". Many firms, which are primarily focused on using digital capabilities to achieve leadership in the customer experience, do not pay sufficient attention to the other side of the coin: the employee experience, an important part of which is their risk culture. After all, risk culture encompasses collective thinking and a shared set of values that shape the daily behaviour of bank employees. It is embedded in the DNA of how a bank operates and manages risks [4].

The aim of the study is to analyse and substantiate the role of risk culture as a key element of a bank's digital DNA, ensuring its sustainable development in the context of active digital transformation. The study focuses on defining the essence and components of the bank's digital DNA, analysing the impact of risk culture on its formation and functioning, and developing methodological approaches to assessing the effectiveness of risk culture based on a process-oriented approach.

1. Content and structure of the bank's digital DNA

The global banking sector is currently navigating an era of unprecedented structural realignment, where the traditional paradigms of financial intermediation are being superseded by a pervasive digital architecture. This transition, often characterized as digital transformation, has evolved beyond the mere implementation of front-end applications or the automation of back-office functions. It now necessitates the cultivation of a "digital DNA" – a fundamental reconfiguration of the institutional essence that integrates technology, data, strategy, and values into a cohesive, self-evolving organism [5].

The concept of digital DNA represents the highest stage of maturity in the evolutionary trajectory of financial institutions. While early stages of digitalization focused on the emergence of digital channels and the implementation of isolated digital products, the contemporary objective is the total enterprise reinvention, where "digital" is no longer a separate division but is marbled throughout the entire organization. This stage involves a systemic paradigm change in management processes, business models, and regulatory interactions [6]. The digital DNA of a bank is not a static set of technologies but a comprehensive management system for the integration of innovation, providing a new coordinate system for strategic decision-making throughout the bank's life cycle.

Traditional digital transformation often failed because firms focused on digital capabilities to enhance customer experience without addressing the internal "employee experience", of which risk-culture is a critical component. To be digital requires a shift toward a tech-enabled mindset where change is not a side initiative but the core strategy. This transformation is supported by a "Digital Core" – a primary source of competitive advantage consisting of cloud-based infrastructure, advanced data platforms, and artificial intelligence (AI) [7]. Research [8] indicates that organizations with digital DNA embedded into their structure can achieve digital maturity goals significantly better than their peers.

Table 1. A comparative analysis of the traditional banking model and a bank's digital DNA.

Component	Traditional Banking Model	Bank's Digital DNA
Values and Mission	Profit-centric; risk-averse; siloed responsibility.	Purpose-driven; ESG-integrated; collective accountability.
Strategy	Technology as a support function; IT as a cost center.	Reinvention as strategy; technology as a growth engine.
Technologies	Legacy mainframes; fragmented apps; manual processing.	Cloud-native; AI/ML-driven; blockchain-enabled; API-first.
Data Architecture	Siloed databases; historical reporting; manual cleanup.	Real-time analytics; data-as-a-product; unified data lake.
Risk-Culture	Compliance-based; reactive; bureaucratic.	Proactive; innovative; "fail-fast" but secure; integrated.

A source: compiled from [7-10].

The integration of these components allows a bank to move faster end-to-end, removing departmental barriers that traditionally slow down innovation. The result is an organization that can anticipate customer needs with precision, moving from reactive service to predictive engagement.[9]

Scientific works [11, 12] identify five main stages of banking business digitalisation:

1. The emergence of digital channels.
2. Creation and implementation of digital products.
3. Changing business models of banks.
4. Creation of artificial intelligence.
5. Building digital DNA.

These stages reflect the evolution of the banking sector in the context of digital transformation, where each subsequent stage builds on the achievements of the previous one, creating a comprehensive digital ecosystem.

At present, the improvement of bank digitalisation management is based on the implementation of the concept of "digital DNA" of the bank [13], which is based on a comprehensive management system for the integration of new technologies and provides for the establishment of a new coordinate system for making strategic decisions throughout the bank's life cycle, in particular

1. Revision of the bank's business model and operating model - aims to increase the level of product digitalisation to improve the bank's performance.
2. Building an ecosystem of partnerships with companies that create new digital innovations.
3. Modernisation of customer interaction, which involves a transition to a customer-centric approach in the development of services and a focus on comprehensive customer service rather than the sale of individual products.
4. Formation of the data architecture of the bank and all its divisions to ensure flexible and multifunctional use.

The digital DNA of the bank (Table 1) includes the integration of new technologies, such as artificial intelligence, machine learning, and blockchain, to improve the efficiency of processes and customer interaction. Researchers [9, 10] emphasise that the introduction of such technologies requires a corresponding transformation of corporate culture focused on understanding and minimising risks. After all, the digitalisation of the banking sector, despite its many advantages, carries a number of significant risks, including cybersecurity (hacker attacks, viruses and malware, social engineering), operational risks (software errors, equipment failures, human errors), reputational risks (loss of customer confidence, outflow of funds), legal risks (non-compliance with regulatory requirements, lawsuits), etc.

2. Bank's risk-culture and its maturity stages

The role of risk-culture as a driver of digital DNA can be effectively analyzed through the lens of Dynamic Capabilities Theory (DCT) and the Resource-Based View (RBV) [14]. DCT emphasizes a firm's ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments. Risk-culture functions as a higher-order capability that governs the evolution of ordinary operational routines. It enables the bank to sense digital opportunities and threats, seize them through strategic action, and transform its organizational assets to remain aligned with evolving market and regulatory conditions.

According to the RBV, a firm achieves sustained competitive advantage by possessing resources that are valuable, rare, inimitable, and non-substitutable (VRIN). Risk-culture is an intangible

asset that is exceptionally difficult for competitors to replicate because it develops through complex, tradition-bound processes. Research demonstrates that a robust risk-culture significantly enhances non-financial performance, including customer satisfaction and internal business processes [15]. By fostering an environment that encourages innovative behavior within secure guardrails, a bank can translate its technological resources into sustainable results.

A bank's risk-culture is defined as the nature of the perception of the importance of risk management by bank employees, as well as the peculiarities of their behaviour when making decisions under conditions of uncertainty [10]. It goes beyond mere compliance with regulations and encompasses the ingrained mindset and attitudes towards risk throughout the institution. A robust risk-culture is built on trust, transparency, and accountability, permeating every level of the organisation [16].

Digital transformation is changing the approach to risk management in banks, placing new demands on the competence of employees. A high level of digital literacy, analytical thinking, communication skills, teamwork and flexibility are becoming key elements of an effective risk culture. Integrating these skills into professional activities allows banking institutions to minimise risks and maintain stability in the digital environment.

In the context of the digital transformation of the banking sector, risk-culture is of particular importance, as digital technologies simultaneously open up new opportunities and pose potential threats. Given the insufficient level of digital literacy of employees, lack of sufficient resources to invest in new technologies and risk management systems, political instability and economic crises, the basic principles for developing risk-culture in Ukrainian banks can be as follows:

1. Proactive corporate culture - creating an atmosphere where employees are willing to identify, report and prevent risks.
2. Effective control systems - implementation of modern risk monitoring and control systems, including the use of data analytics.
3. Investments in cybersecurity - regular software updates, pentesting, and employee training.
4. Cooperation with the regulator - active participation in the development and implementation of new regulatory requirements of the NBU.
5. Transparency and openness - ensuring transparency of decision-making processes related to risk management.

In the context of forming a bank's risk-culture, it is important to determine the evolutionary stages of its development or, in other words, to model the stages of its maturity. After all, it is the development and formation of a mature risk-culture of a bank that is a basic prerequisite for the evolutionary transformation of the bank's digital DNA.

In detailing the formation of a bank's risk-culture by organizational approach, we believe that the following stages should be distinguished: inception, formation, maturity and full integration of the risk-culture into the overall management system of the bank and its perception as an integral part.

The nascent stage focuses on the formulation of corporate values that contribute to the bank's sustainable development. The methodological basis is a critical analysis of the existing corporate culture and modelling the impact of changes in values on the bank's digital DNA using the following tools: SWOT analysis and tools for monitoring compliance with corporate values. At the organisational level, the risk-culture is localised in the area of internal audit and is limited to compliance measures.

At the formation stage, the focus shifts to the development of a code of conduct and ethics for employees and managers, as well as to consolidating the risk-culture as an integral element of the

bank's digital DNA. Methods include the substantive structuring of risk-culture, parameterisation of its determinants, and quality assessment. The tools are the norms of stakeholder behaviour and means of controlling risk behaviour. Importantly, this stage involves the institutional separation of risk-culture from internal audit, the identification of objects and the development of a quality assessment methodology.

Formalisation and implementation of the risk-culture at all organisational levels of the bank takes place at the maturity stage. This stage is implemented through the formation of risk-culture reporting and the establishment of effective communication by defining the risk-culture policy, reporting forms and intra-bank communication channels. Risk-culture becomes a holistic management entity, subject to internal audit assessment, with clearly defined functions.

The last stage is the comprehensive integration of risk-culture elements into the bank's digital DNA and its overall management system. The postulates of risk-culture are implemented in the activities of all departments through job descriptions, conflict of interest policies, training programmes, etc. At the same time, the risk-culture becomes value-based, with priority given to compliance with the bank's risk appetite, ethical values and reputation.

It is worth emphasising that the most significant transformations in a bank's functioning occur when its risk-culture moves from a mature stage to an integrated one. This applies not only to the inclusion of risk management principles in strategic or top management decision-making, but also to their daily implementation in the digital DNA of the bank, along with all operational processes.

It is also worth noting that the increased demand for transparency, risk-based decision-making and a high level of social responsibility of financial institutions is not only driven by regulators. Market participants, consumers of financial services, and society as a whole also play a significant role in this.

All of these factors combine to make it necessary to actively implement self-regulatory mechanisms in the banking sector. This approach is a key factor in strengthening the bank's ability to ensure sustainable development, even in the face of difficult macroeconomic challenges, which are becoming particularly acute in light of the current unprecedented crisis caused by the global pandemic and military operations.

3. The conceptual foundations of the impact of risk culture on a bank's digital DNA

Given the above, it can be argued that the key factors that determine the risk-culture in the context of ensuring the bank's sustainable development are as follows:

1) the level of risk competence of all employees, including top and middle management;

2) motivation of internal stakeholders to implement a risk-based approach as the basis for professional activity;

3) effectiveness of communications between various structural units of the bank at all levels of management, which involves both vertical and cross-functional interaction;

4) comprehensiveness and efficiency of the internal risk management system.

Thus, risk-culture is an important mechanism that integrates various aspects of bank management through a risk-based approach, contributing to the bank's integrity and flexibility of its digital DNA in response to the challenges of sustainable development. Moreover, it serves as a kind of 'conceptual framework' that forms a strategic vector for improving the bank's operations and enhances the overall efficiency of its functioning. The relationship between the risk-culture and the digital DNA of a bank is shown in the diagram (Fig. 1).

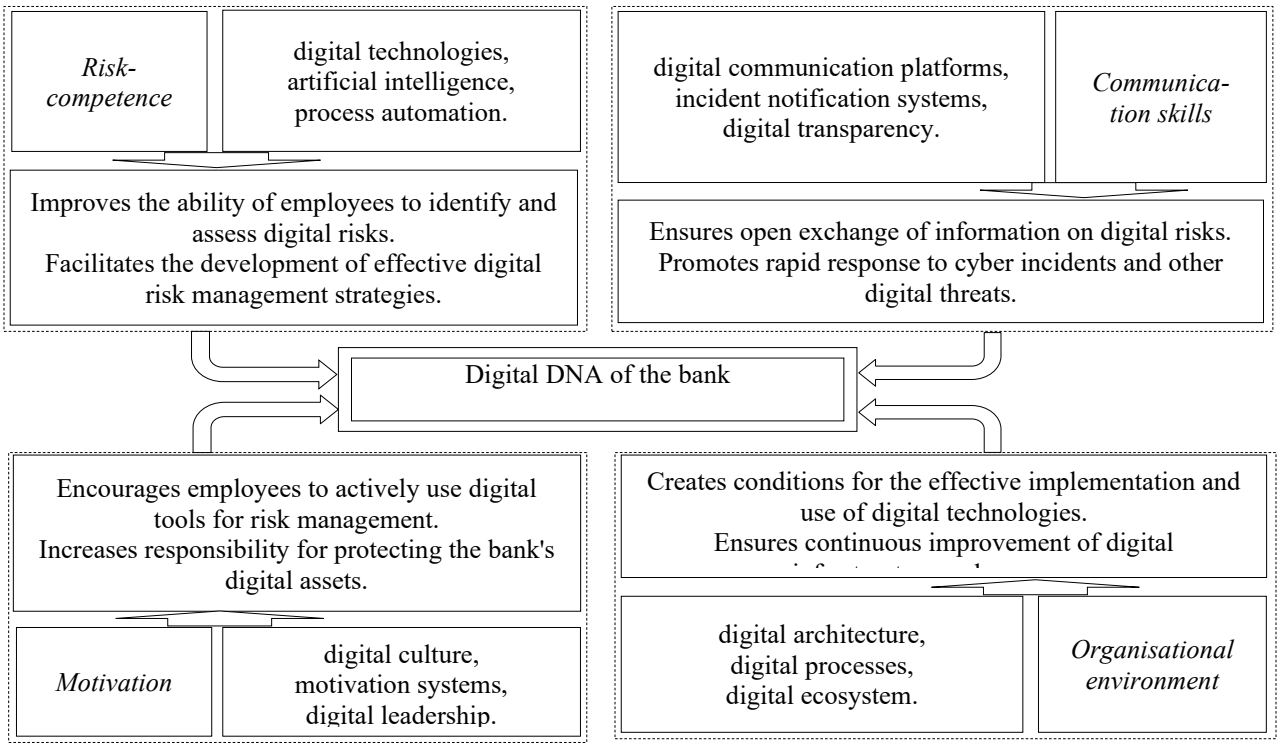

Figure 1. A Map of the impact of risk-culture effects on the bank's digital DNA
A source: [17]

Risk-culture is a key element of a bank's digital DNA, determining its ability to effectively adapt to change and ensure sustainable operation in the context of digital transformation. While its direct impact is on the risk management system, it also shapes strategic approaches to risk management in the digital environment. A robust risk-culture is integrated into the bank's digital architecture, promoting the development of risk-adjusted technological solutions and the formation of risk-aware behaviour of employees in the use of digital tools.

4. Risk-culture: process efficiency

The efficiency of the bank's risk-culture directly depends on the readiness of the entire set of responsible units in the risk management system to continuously improve risk management technologies. As a methodological basis for the applied implementation of continuous improvement of the bank's risk-culture as an element of its digital DNA, it is appropriate to use the Deming-Schuhart cycle [18], the content of which is presented in Fig. 2.:

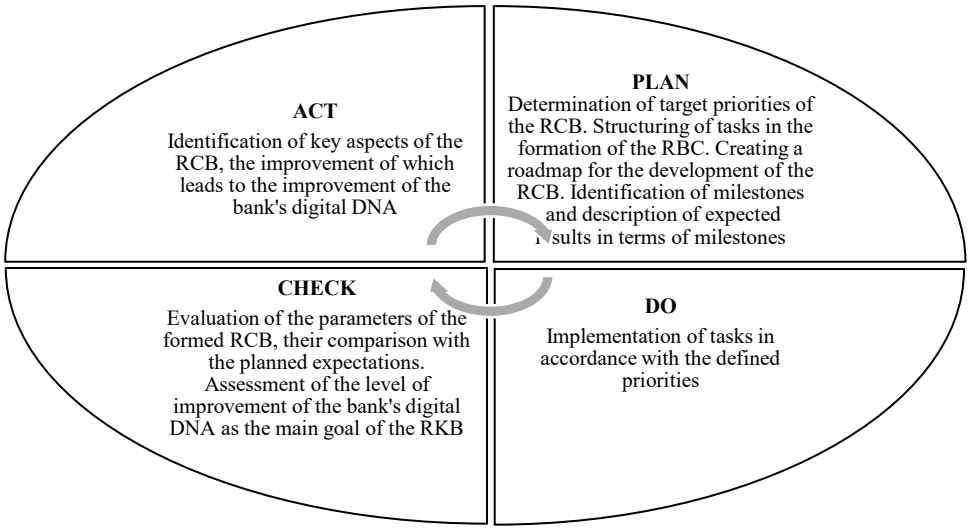

Figure 2. Continuity of formation of the bank's risk-culture (RCB) from the perspective of the Deming-Schuhart process approach.

Authoring

Plan: setting clear, measurable, attainable, relevant and time-bound (SMART) goals for the digital transformation of risk management; developing strategies and identifying specific steps and resources required to achieve the goals; areas of digital integration, taking into account cybersecurity and data protection.

Do: implementing technology (installing software, setting up data analytics systems, or launching digital platforms); conducting training programmes for employees to familiarise them with new tools and processes and ensure effective communication; and implementing digital in a business continuity environment.

Check: monitoring and analysis using digital tools to collect and analyse data on the effectiveness of implemented measures; use of analytical tools to assess changes in the level of risks after the introduction of new technologies; identification of potential shortcomings or new risks of digital transformation; development of digital metrics and indicators to assess the effectiveness of risk-culture.

Act: making the necessary changes to strategies, processes or technological solutions; creating a culture of continuous learning and development in digital risk management; using digital tools to automate the process of making changes and track their effectiveness; ensuring continuous improvement of the digital infrastructure.

The responsibility for the implementation of the defined tasks at the ACT and PLAN stages should rest with the risk management unit and the supervisory board committee dealing with risk management issues. The main elements of the bank's risk-culture should be enshrined in the risk management policy, and measures to develop or improve it should be reflected in the risk management strategy. The bank's management board is responsible for implementing measures to form the bank's risk-culture (stage DO), which is obliged to inform all structural units and employees about the key priorities of the risk-culture and its importance for achieving the bank's

strategic goals. Finally, the risk management unit assesses the effectiveness of the implemented risk-culture development measures (the 'CHECK' stage), and the quality of these measures and their compliance with the expected risk management results are discussed in the bank's supervisory board committee responsible for risk management.

Continuous development of the bank's risk-culture based on the Deming-Schuchart process approach is a critical element of success in the context of digital transformation. Integration of the PDCA cycle into the digital DNA of the bank allows to create an effective risk management system that ensures stability, success and competitiveness of the bank in the financial services market. The starting point for building an effective risk-culture should be to focus on internal controls, such as ethical standards and the formulation of organisational norms for handling failure. In order to achieve a common understanding of appropriate and ethically acceptable risk behaviour, each bank should align its controls over actions (organisational structure, accountability and supervision), controls over results (incentive systems) and controls over personnel (hiring and training, communication, knowledge and characteristics of personnel) with each other [19].

5. Metrics of risk-culture

The formation of metrics for assessing the effectiveness of risk-culture is critical to ensuring the bank's sustainable development in a dynamic market environment. This allows to quantify the level of risk-culture development in the bank, provides the possibility of regular monitoring and tracking of the dynamics of changes for timely identification of potential problems and taking corrective measures, increases the transparency of the business model and facilitates responsible, informed management decisions.

Metrics for assessing the risk-culture in the bank's digital DNA are based on a set of quantitative and qualitative indicators that reflect the level of risk management, their integration into business processes and the impact on the bank's long-term sustainable development. The main metrics can be divided into cultural and behavioural, financial and economic, management efficiency, digital and technological. These categories are explained in Table 2.

Table 2. Metrics for assessing risk-culture in the bank's digital DNA.

Cultural and behavioural metrics	Risk management performance metrics	Financial and economic metrics	Digital and technological metrics
Employee Risk Awareness Index. Percentage of employees trained in risk management. Risk transparency index. Number of identified and eliminated violations of risk management policies.	The number and level of incidents related to breaches of internal risk procedures. Share of decisions that have undergone risk assessment before implementation. Frequency of updating risk strategies. Level of compliance with regulatory requirements and risk management standards.	The level of risk provisions. The bank's credit rating. Dynamics of the risk/return ratio. Share of ESG-oriented assets in the total portfolio.	The level of automation of risk management processes. The number of cyber incidents and the level of their successful neutralisation. Response time to identified risks in the digital environment. Digital Compliance Index.

A source: [20]

It should be added that the Financial Stability Board proposes to assess a bank's risk-culture in four key areas: senior management involvement, accountability, communication effectiveness, and incentives [21]. These areas determine the extent to which a bank integrates risk-culture into its operations and ensures effective risk management.

The indicative approach involves assessing a bank by a set of characteristics that allow determining its level of risk management maturity. For example, the assessment of management involvement considers the responsibility of the supervisory board, compliance with the risk appetite and control over the implemented risk-culture based on the following indicators: the share of transactions exceeding the established limits; the share of strategic decisions aimed at developing the risk-culture; and the level of compliance of managers with risk management requirements.

Reporting in a bank covers the quality of interaction between departments and employee awareness of risks. An important element is the existence of mechanisms for self-identification of problems that allow timely response to violations. This area can be assessed by analysing the proportion of sanctions for violations of the code of conduct, the number of reports of unacceptable behaviour, and the level of responsibility of business units for risk management. It is also necessary to assess the compliance of internal audits and inspection reports of regulators, the effectiveness of delegation of responsibility and the level of self-control of business process managers.

Assessing the effectiveness of communication involves analysing the bank's openness to discussing risks, the independence of control units and the overall effectiveness of risk management. Indicators include the number of cross-functional meetings, the level of employee awareness of risks and the use of communication channels to communicate risk information, the availability of a system of regular staff surveys on understanding the risk-culture, and the number of management communication initiatives aimed at aligning the bank's activities in the face of change.

The system of rewards and penalties should be closely linked to the quality of risk management at all levels of the bank. Assessment of the effectiveness of incentives may include an analysis of the share of incentives that directly depend on compliance with risk appetite, staff participation in risk management training, and the level of training of managers to perform control functions. Other relevant indicators include the proportion of executives who receive risk management training, the ratio of employees in business units to those in control functions, and the inclusion of risk-culture assessment in the process of appointing executives.Thus, the assessment of a bank's risk-culture should be comprehensive, covering all key aspects of its formation and functioning.

The use of these metrics allows a sustainable development bank to assess and improve the risk-culture integrated into its digital DNA, which contributes to stability and long-term sustainability, as a developed risk-culture is an important component of the bank's digital DNA, which affects its resilience and ability to adapt to challenges. The integration of an indicative approach to assessing risk-culture allows banks to improve the quality of risk management, ensure effective communication, and create a transparent system for incentivising responsible behaviour.

6. ESG-Communication: the conscience of the digital DNA

As banks integrate digital technologies, they must also manage their environmental, social, and governance (ESG) responsibilities. Effective ESG-communication is becoming a critical factor for

long-term sustainability and competitiveness, especially in the context of Ukraine's European integration.

Integrating ESG principles into a bank's strategy and business model requires not only internal transformations but also transparent and effective communication with stakeholders. The findings of the study provide a comprehensive overview of the nature, stages and tools of ESG communication in the banking sector, as well as highlighting its significance in the context of European integration.

ESG communication is a strategic and transparent process of disclosure, explanation and interaction between financial institutions and stakeholders regarding the environmental, social and governance responsibilities of banks, as well as the impact of their financial activities and investments on these factors. Moreover, the proposed definition goes beyond the scope of purely quantitative reporting, encompassing the formulation of the bank's ESG vision, the integration of this vision into strategic planning, and the disclosure of its consistent commitment to the concept of sustainable and responsible banking for all stakeholders. Therefore, ESG communication should include the following aspects:

1. Environmental – communication regarding the bank's impact on climate change (carbon footprint), energy use, emissions, resource conservation and sustainable lending, covering information on the re-evaluation of investments, the setting of targets aligned with international agreements (such as the Paris Agreement), and support for environmental projects.
2. Social – disclosure of information regarding the bank's impact on communities, ethical labour practices, human rights, diversity and inclusion (D&I), as well as support for socially vulnerable groups, including details of partnerships with non-profit organisations, priority lending to small businesses, and initiatives aimed at improving financial literacy.
3. Governance – communication regarding ethical principles of banking, compliance with regulatory requirements, anti-corruption policies, diversity of the board of directors, transparency of reporting, accountability and responsibility for instances of greenwashing or business miscalculations.

Implementing effective ESG communication is a systematic process comprising seven interrelated stages. This phased model, summarised based on an analysis of literature and existing practices, provides a structured approach to integrating ESG communication into a bank's business model (Table 3).

Table 3. Stages of implementing ESG communication into a bank's business model

Stage	Stage name	Key actions
1	Getting started – vision, objectives and governance	Defining the bank's overall approach to ESG and its acceptable risk level; setting clear, measurable (SMART) ESG goals and targets aligned with the bank's mission and values; forming a broad cross-functional team comprising representatives from various departments, including senior management; defining leadership roles (e.g., Head of Sustainability); Integrating ESG into the bank's governance structure, including board oversight and management accountability.
2	Stakeholder analysis and materiality assessment	Identification of key stakeholders (investors, customers, employees, regulators, communities, suppliers); analysis of their expectations and concerns regarding ESG issues; conducting a materiality assessment to identify priority ESG issues for the bank and its stakeholders (using international SASB and GRI standards); actively engaging stakeholders in the process through surveys, interviews and focus groups.

3	Development of an ESG communication strategy	Identification of key messages that align with the bank's mission and values, highlighting ESG achievements and initiatives with specific examples and figures; identification of target audiences for different messages and tailoring communications to their needs; selecting appropriate communication channels (sustainability reports, annual reports, website, social media, press releases, investor conferences, internal communications); developing a clear ESG communication plan aligned with the bank's overall strategy.
4	Data collection, measurement and reporting frameworks	Identifying relevant ESG reporting frameworks and standards (GRI, SASB, TCFD, CSRD, SFDR, UN Sustainable Development Goals); establishing robust processes for collecting, managing and verifying ESG data from various internal and external sources; addressing data gaps and ensuring data accuracy and integrity; establishing key performance indicators (KPIs) to measure progress towards ESG targets; considering ESG ratings and indices as benchmarks for performance assessment.
5	Content Development and Transparency	Creating compelling narratives and authentic stories that go beyond simple data presentation, highlighting the impact of the bank's ESG initiatives and emphasising the human aspect; ensuring transparency by providing honest and clear information on both successes and shortcomings in ESG performance; Avoiding greenwashing by backing up claims with data and specific examples.
6	Communication and Engagement	Implementing the communication plan through selected channels, ensuring consistency in messaging; adopting an 'always-on' approach, providing regular updates on ESG initiatives and achievements throughout the year; actively engaging stakeholders to discuss results and gather feedback; ensuring internal communication and employee support by clearly communicating the bank's ESG strategy, individual roles and progress.
7	Monitoring, evaluation and continuous improvement	Establishing KPIs to track the success of ESG communication efforts (level of stakeholder engagement, media coverage, changes in ESG ratings); regular monitoring and evaluation of the communication strategy's effectiveness based on feedback and results; adapting and refining the ESG strategy and communication plan based on changes in regulatory requirements, stakeholder expectations and performance data..

A sourse: [10].

Managing ESG communication requires not only an understanding of the key stages, but also the ability to anticipate potential challenges that may arise during implementation. To effectively integrate ESG principles into a bank's corporate culture and business model, it is necessary to account for potential gaps and inconsistencies in data at all stages of implementation – from collection and management to verification of its accuracy. One of the significant challenges is the need to navigate numerous international and national standards (GRI, SASB, TCFD, CSRD, SFDR), as well as to constantly adapt to changing legislation. Maintaining stakeholder trust and avoiding accusations of greenwashing (providing false or misleading information about environmental performance) requires the utmost honesty and the substantiation of all claims with reliable data [5]. Another challenge is the need to quantitatively assess the impact and return on investment in ESG initiatives, as well as the effectiveness of communication. This requires the involvement of all the bank's departments in implementing the overall ESG strategy.

However, despite the challenges, effective ESG communication generates significant benefits for banks, including:

- enhancing reputation and brand image;
- attracting and retaining investors;
- developing and retaining talented staff; improving customer relations and strengthening their trust and loyalty; mitigating risks and ensuring regulatory compliance;

– opening up new business opportunities and collaborations.

The proposed phased model for implementing ESG communication systematises existing approaches, providing banks with a clear roadmap. In particular, the focus on the "Launch – vision, objectives and governance" phase is of critical importance, as it is at this stage that the foundations are laid for the authenticity and effectiveness of subsequent communications.

As noted in the National Bank of Ukraine's "White Paper" [22], harmonisation of legislation with the EU is not merely a requirement, but a strategic opportunity for Ukrainian banks to integrate into the single financial area. This study emphasises that international regulations not only establish new reporting standards but also require a fundamental rethinking of approaches to data collection, management and transparency, which directly influences communication strategy. Compliance with these requirements becomes a competitive advantage, enabling the attraction of European investment and the strengthening of an international image.

In today's banking sector, operating amid growing global attention to sustainable development, effective ESG communication is not merely a trend, but a critically important factor for long-term sustainability and competitiveness. A comprehensive analysis demonstrates that ESG communication is a strategic process that goes beyond standard reporting, encompassing transparent disclosure and the integration of an ESG vision into all of the bank's business processes. The study confirms that the implementation of effective ESG communication generates a number of strategic advantages. It strengthens stakeholder trust, improves reputation and brand image, facilitates investment attraction, increases customer loyalty and helps minimise risks associated with regulatory requirements and reputational damage. Furthermore, it is argued that a phased model for implementing ESG communication, comprising seven key steps – from initiation to continuous monitoring – is essential to ensure its consistency and authenticity.

7. DORA and the 2024 Basel Core Principles as a basic regulatory imperatives

The regulatory landscape in 2024 and 2025 has become a primary external driver forcing the integration of risk-culture into the bank's digital DNA. The introduction of the Digital Operational Resilience Act (DORA) [23] in the European Union and the 2024 revision of the Basel Core Principles for Effective Banking Supervision (BCPs) [24] mark a shift from traditional risk management to holistic digital resilience.

DORA is a landmark regulation designed to ensure that financial institutions can withstand, respond to, and recover from ICT-related disruptions. It mandates that resilience be embedded into the "DNA" of the organization rather than being treated as a separate compliance chore. DORA establishes five key pillars: ICT risk management, incident reporting, operational resilience testing, third-party risk management, and information sharing.

The implementation of DORA requires significant cultural shifts. Banks must move toward a "security-first" culture where every employee is part of the digital defense system. For mid-tier banks, DORA compliance often necessitates adopting closed-source data management solutions to guarantee the security and accessibility of critical data. Non-compliance with DORA carries severe financial and reputational consequences, including fines of up to 2% of global annual turnover, which underscores the necessity of a resilient risk-culture.

The 2024 BCP updates explicitly embed digitalization and climate-related financial risks into supervisory practices for the first time. These revisions preserve the foundational architecture of the principles while introducing granular expectations for cybersecurity, business continuity, and the governance of digital tools. The revised principles raise the bar for both banks and

supervisors, requiring them to address the systemic footprint of digital finance and non-bank financial intermediation. This regulatory evolution forces banks to adopt a forward-looking risk-culture that can navigate the "perpetual motion" of the modern financial environment.

Table 4. The regulatory framework and its impact on the transformation of banks' risk culture.

Regulatory Framework	Focus Area	Impact on Risk-Culture
DORA (EU)	Digital operational resilience and ICT security.	Shifts culture from checkbox compliance to "resilience-by-design".
Revised BCP (2024)	Digital and climate-related financial risks.	Requires forward-looking provisioning and ICT risk expertise.
CRR III / CRD VI	Internal governance and management accountability.	Strengthens "fit-and-proper" assessments and role mapping.
CSRD / ESRS (EU)	Sustainability and ESG reporting.	Demands transparent communication of social and environmental impact.

A sourse [23-25]

The rapid adoption of Artificial Intelligence, and particularly Generative AI (GenAI), is fundamentally reshaping the bank's digital DNA. By 2025, AI is expected to drive up to a 15-percentage-point improvement in bank efficiency ratios through revenue growth and cost transformation. However, this technological leap also introduces "agentic" risks—autonomous systems that can act, learn, and reason with limited human oversight.

To manage the risks associated with AI, banks must implement clear governance frameworks that prioritize transparency, fairness, and explainability. Chief Risk Officers (CROs) are now expected to spearhead the design of AI risk management mechanisms, including risk-based triaging of AI processes. The AI-defined future necessitates a "human-in-the-loop" model, where risk functions are tech-driven but human-supervised.

As day-to-day operational tasks like credit scoring and fraud detection become fully automated, the role of risk managers shifts from execution to oversight. This transition requires a new talent mix, including data scientists, AI specialists, and ethics stewards who can ensure that AI-driven decisions remain consistent with enterprise values. The upskilling of the workforce is critical; moving too slowly to adopt AI can result in competitive disadvantage, while moving too quickly without proper risk management can lead to catastrophic operational failures.

Banks are initially deploying AI agents in functions like transaction monitoring and internal process automation where deterministic models offer greater auditability. However, the use of Large Language Models (LLMs) in high-risk functions like credit provision requires sophisticated "interpretable" tools like LIME and SHAP to explain agent actions. A mature risk-culture ensures that these agents are not just efficient but are also compliant with the stringent regulatory expectations for auditability and fairness.

In Ukraine, the development of Supervisory Technology (SupTech) and Regulatory Technology (RegTech) has become a central component of the financial sector's digital DNA. The wartime

pressures in Ukraine have accelerated the shift toward automated compliance. The NBU has developed a sophisticated three-pillar SupTech architecture designed to guarantee the continuity of financial services even under extreme conditions [26].

1. Incident-Reporting API: an API portal that allows banks to transmit structured event logs and resilience test results to a central data lake. This system enables the NBU to specifies exact incident attributes, from the "T-moment" (first symptom) to the "R-moment" (response).
2. Regulatory Sandbox: a secure environment for testing new digital solutions and RegTech tools without immediate regulatory consequences, fostering innovation while maintaining control.
3. Real-Time Supervisory Dashboard: a centralized platform built on microservice architecture, integrating graph databases and BERT-based semantic parsers. This dashboard enables supervisors to monitor the cyber-incident landscape and risk scores in near real-time, reducing average incident-detection time from 27 to 9 minutes in pilot trials.

This technological core allows for cost-of-compliance-as-a-service models, which are particularly valuable for institutions facing financial and staffing constraints in a transitional economy. However, the success of these tools relies on a security-minded organizational culture that ensures data integrity and timely reporting.

Summary and Conclusions

This study has substantiated the crucial role of risk-culture as the primary driver of digital transformation within the banking sector, emphasizing its necessary integration into a bank's digital DNA – a complex synthesis of technology, data architecture, strategy, and organizational values. It was found that modern digitalization has evolved beyond mere front-end automation toward a pervasive digital architecture where "digital" is "marbled" throughout the entire institution. Within this framework, risk-culture functions as a high-order dynamic capability that enables banks to sense digital threats, seize innovation opportunities, and reconfigure organizational assets to maintain stability. The research demonstrates that risk-culture directly shapes strategic approaches to risk management by fostering an environment that encourages innovative behavior within secure, proactive guardrails.

The development of this integrated risk-culture is not instantaneous but progresses through distinct evolutionary stages – from inception and formation to maturity and full integration – where the principles of risk management eventually become an inseparable part of daily operational DNA. To ensure the continuous improvement of this culture, the effective utilization of the Deming-Schuhart (PDCA) process approach provides a viable methodology for aligning digital transformation goals with cybersecurity and data protection requirements. Central to this evolution is the implementation of comprehensive metrics covering cultural, behavioral, financial, and technological dimensions, which allow for the quantifiable monitoring and enhancement of risk-culture effectiveness in a dynamic market environment.

As banks navigate this digital transition, ESG communication has emerged as a critical conscience of the digital DNA, particularly in the context of Ukraine's European integration. Effective ESG communication is identified as a strategic process that moves beyond quantitative reporting to a transparent disclosure of environmental, social, and governance responsibilities. By integrating ESG principles into the business model through a structured seven-stage phased model, banks can strengthen stakeholder trust, attract sustainable investment, and mitigate risks

such as greenwashing. This transparency is further reinforced by the shifting regulatory landscape of 2024 and 2025, where mandates like the Digital Operational Resilience Act (DORA) and the revised Basel Core Principles (BCPs) shift the paradigm toward resilience-by-design. These frameworks necessitate a security-first culture where ICT risk management and digital resilience are embedded into the institutional essence rather than treated as isolated compliance tasks.

Furthermore, the rapid adoption of Artificial Intelligence and Generative AI is fundamentally reshaping the technological core of the banking sector, introducing significant efficiency gains alongside new agentic risks. Managing these risks requires a "human-in-the-loop" model, where automated processes like credit scoring or fraud detection remain under human supervision to ensure transparency, fairness, and accountability. This transition demands a new talent mix and the continuous upskilling of employees to handle sophisticated AI-driven tools. In Ukraine, this technological advancement is complemented by the development of SupTech and RegTech architectures, such as incident-reporting APIs and real-time supervisory dashboards, which automate compliance and enhance sector resilience even under wartime pressures.

In conclusion, the study finds that ensuring the sustainable development of the banking sector requires more than just technological advancement; it necessitates the deep embedding of a robust risk-culture across all levels of the organizational structure. By combining advanced technologies like blockchain and AI with a value-based risk-culture and a proactive approach to ESG and regulatory compliance, banks can successfully adapt to the challenges of the digital age. This comprehensive approach serves as a model for implementing sustainable, secure, and transparent digital financial ecosystems that can withstand macroeconomic challenges and meet the increasing demands of society.

Declarations

The manuscript has not been submitted to any other journal or conference.

Study Limitations

There are no limitations that could affect the results of the study.

Acknowledgments

The author would like to thank for the support staff and experienced people who participated in this study by sharing their invaluable knowledge and experience. Their cooperation and openness contributed greatly to the depth and richness of the research results.

Competing Interests

The authors declare no competing interests.

Funding Source

This research was conducted without support from external funding.

Ethical Standards

The research meets all ethical guidelines, including adherence to the legal requirements of the study country.

REFERENCES

1. National Bank of Ukraine. (2021, July). Concept of development of innovative supervisory and regulatory technologies [Consultation document]. https://bank.gov.ua/ua/news/all/kontseptsiya-rozvitku-innovatsiynih-naglyadovih-ta-regulyatornih-tehnologiy
2. Ministry of Digital Transformation of Ukraine. (2022). Diia Project. https://plan2.diia.gov.ua/
3. Tahiri, S. (2022). The impact of digitalization on firms' business models: Opportunities and limitations for digital leader. Journal of Advanced Research in Leadership, 1(1), 13–32. https://doi.org/10.33422/jarl.v1i1.173
4. Elderson, F. (2023, September 19). Treading softly yet boldly: How culture drives risk in banks and what supervisors can do about it. European Central Bank. https://www.bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp230919~589c61455b.en.html
5. Gosling, W. (2014). Building your digital DNA: Lessons from digital leaders. Deloitte UK. https://www.scribd.com/document/365371551/Deloitte-Uk-Building-Your-Digital-Dna
6. Di Vaio, A., Latif, B., Gunarathne, N., Gupta, M., & D'Adamo, I. (2023). Digitalization and artificial knowledge for accountability in SCM: A systematic literature review. Journal of Enterprise Information Management, 37(2), 606–672. https://doi.org/10.1108/JEIM-08-2022-0275
7. Abad, M. S. S., Jalilvand, M. R., Sharif, M., & Khani, N. (2024). Understanding dynamic capabilities for digital transformation: A literature review and future research directions. Journal of Innovation & Knowledge, 9(2), Article 100481. https://doi.org/10.1016/j.jik.2024.100481
8. Mariani, J., Murphy, T. J., Eggers, W. D., & Turley, C. (2023, June 14). The digital transformation of government: Preparing for the next generation of public services. Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/government-digital-transformation-strategy.html
9. Kaplan, R. S., & Mikes, A. (2016). Risk management – the revealing hand. Journal of Applied Corporate Finance, 28(1), 8–18. https://www.hbs.edu/faculty/Pages/item.aspx?num=51099
10. Vovchenko, O. S., & Karpenko, Ye. A. (2025). ESG-communication management in the banking sector: Challenges and advantages. Problems of Modern Transformations. Series: Economics and Management, (20). https://doi.org/10.54929/2786-5738-2025-20-08-03
11. Broeders, H., & Khanna, S. (2015). Strategic choices for banks in the digital age. McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/strategic-choices-for-banks-in-the-digital-age
12. Kochuma, I. (2021). The impact of digitalisation of the banking sector on employment transformation in modern conditions. Financial Space, 4(44), 149–158. https://doi.org/10.18371/fp.4(44).2021.149158
13. Kasich, A., & Naumkina, I. (2021). Digitalization processes as an integral part of modern banking management. Economy and Society, (28). https://doi.org/10.32782/2524-0072/2021-28-1

14. Tanveer, M. (2026). FinTech-enabled digital transformation for sustainable performance: The strategic role of dynamic capabilities. Frontiers in Human Dynamics, 8, Article 1747642. https://doi.org/10.3389/fhumd.2026.1747642
15. Oziri, V., & Knox, S. (2025). The strategic role of risk culture in enhancing innovation and non-financial performance: Evidence from the insurance sector. Journal of Risk Research, 28(7), 705–730. https://doi.org/10.1080/13669877.2025.2553083
16. Danik, N., & Torlopov, A. (2024). The impact of digital transformation on the banking sector of Ukraine. International Science Journal of Management, Economics & Finance, (3), 95–103. https://doi.org/10.46299/j.isjmef.20240303.09
17. Vovchenko, O. (2023). ESG-strategy as a basis for sustainability risk management in banks. Economy and Society, (50). https://economyandsociety.in.ua/index.php/journal/article/view/2458/2377
18. The W. Edwards Deming Institute. (2024). PDSA Cycle. https://deming.org/explore/pdsa/
19. Financial Stability Board. (2014, April 7). Guidance on supervisory interaction with financial institutions on risk-culture: A framework for assessing risk-culture. https://www.fsb.org/uploads/140407.pdf
20. Vovchenko, O. (2024). Risk-culture in the bank's digital DNA: The foundation of sustainable development. In Digital Economy and IT: Trends and Perspectives 2024: Proceedings of the International Scientific and Practical Conference (pp. 50–52). Yuri Kondratyuk Poltava Polytechnic National University.
21. Basel Committee on Banking Supervision. (2023, July 6). Core principles for effective banking supervision [Consultative document]. Bank for International Settlements. https://www.bis.org/bcbs/publ/d551.htm
22. National Bank of Ukraine. (2025). White paper: Main directions for the development of the financial sector of Ukraine. https://bank.gov.ua/admin_uploads/article/Bila_knyga_2025_fin.pdf?v=13
23. European Insurance and Occupational Pensions Authority. (2024). Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
24. Basel Committee on Banking Supervision. (2024). Core principles for effective banking supervision. Bank for International Settlements. https://www.bis.org/bcbs/publ/d581.pdf
25. European Banking Authority. (2025). Consultation on EBA/CP/2025/20: Draft guidelines on the prudential supervision of digital transformation. https://banking.vision/en/consultation-on-eba-cp-2025-20/
26. Taranenko, A. (2025). Innovative mechanisms of state regulation of information security of financial institutions in Ukraine in the context of DORA implementation and SupTech tools development. Visegrad Journal on Human Rights, (2), 165–171. https://doi.org/10.61345/1339-7915.2025.2.26.