Research paper / Оригинальная статья
https://doi.org/10.51176/1997-9967-2026-3-70-88
МРНТИ 05.73.55
JEL: G01, G21, G32

Check for updates

CC BY 4.0

Corporate Security and Financial Stability of Ukrainian Banks under Crisis Conditions

Anastasiia Poltorak[a]*, Hanna Fedosieieva[a], Olena Bodnar[a], Anna Sukhorukova[a], Andrii Ahafonov[a]

[a] *Mykolaiv National Agrarian University, 9 Georgiy Gongadze Str., 54008, Mykolaiv, Ukraine*

For citation: Poltorak, A., Fedosieieva, H., Bodnar, O., Sukhorukova, A. & Ahafonov, A. (2026). Corporate Security and Financial Stability of Ukrainian Banks under Crisis Conditions. Economy: strategy and practice, 21(3), 70-88. https://doi.org/10.51176/1997-9967-2026-3-70-88

ABSTRACT

In the context of growing challenges to the security of the banking sector during Ukraine's post-war economic transformation, it has become necessary to rethink approaches to the strategic management of banks with an emphasis on security factors. This study addresses the insufficient integration of corporate security factors into comprehensive models for assessing and managing the financial stability of commercial banks under wartime conditions. The methodological framework combined structural and functional analysis, scenario forecasting, and econometric modeling. The initial information base consisted of data from the National Bank of Ukraine, financial and non-financial statements of 10 banks, materials from international rating agencies, and publicly available corporate data. The results revealed significant heterogeneity in the financial parameters of the banks under study. The highest capital adequacy ratios were recorded at Credit Agricole Bank – 24.5% and Raiffeisen Bank – 23.8%, while Ukreximbank's figure was 16.1%. The share of non-performing loans reached 28.9% at Ukreximbank and 23.7% at Oschadbank. Universal Bank reported the highest return on assets – 1.1%, and the level of credit risk coverage by reserves at PrivatBank and Credit Agricole Bank was 98% each. Standardized sensitivity coefficients between the corporate security index and ROA increase from 0.47 to 0.78, and with CAR — from 0.33 to 0.66, while an inverse relationship remains for NPL, ranging from −0.52 to −0.70. The results obtained can be used by regulatory bodies, the management of banking institutions, and analytical organizations when developing policies to ensure financial security in the context of the structural transformation of the economy.

KEYWORDS: Financial Economy, Financial Stability, Bank, Banking Sector, Banking Stability, Cybersecurity, Ukraine

CONFLICT OF INTEREST: the authors declare that there is no conflict of interest

FINANCIAL SUPPORT: the study was not sponsored (own resources).

Article history:
Received 09 July 2026
Accepted 25 August 2026
Published 30 September 2026

*** Corresponding author: Poltorak A.** – Full Doctor, Head of the Department of Management, Business and Administration, Mykolaiv National Agrarian University, 9 Georgiy Gongadze Str., 54008, Mykolaiv, Ukraine, +380 512 709 331, email: anastasiiapoltorak7@gmail.com

Корпоративная безопасность и финансовая устойчивость банков Украины в условиях кризиса

Полторак А.[a]*, Федосеева А.[a], Боднар Е.[a], Сухорукова А.[a], Агафонов А.[a]

[a] *Николаевский национальный аграрный университет, ул. Георгия Гонгадзе 9, 54008, Николаев, Украина*

Для цитирования: Полторак А., Федосеева А., Боднар Е., Сухорукова А., Агафонов А. (2026). Корпоративная безопасность и финансовая устойчивость банков Украины в условиях кризиса. Экономика: стратегия и практика, 21(3), 70-88. https://doi.org/10.51176/1997-9967-2026-3-70-88

АННОТАЦИЯ

В условиях растущих вызовов безопасности банковского сектора в период послевоенной экономической трансформации Украины возникла необходимость переосмысления подходов к стратегическому управлению банками с уделением особого внимания факторам безопасности. В данном исследовании рассматривается проблема недостаточной интеграции факторов корпоративной безопасности в комплексные модели оценки и управления финансовой стабильностью коммерческих банков в условиях военного времени. Методологическая основа сочетала структурный и функциональный анализ, сценарное прогнозирование и эконометрическое моделирование. Исходную информационную базу составили данные Национального банка Украины, финансовая и нефинансовая отчетность 10 банков, материалы международных рейтинговых агентств и открытые корпоративные данные. Результаты показали существенную неоднородность финансовых параметров исследуемых банков. Наиболее высокие значения достаточности капитала зафиксированы у Credit Agricole Bank – 24.5% и Raiffeisen Bank – 23.8%, тогда как у Ukreximbank показатель составил 16.1%. Доля неработающих кредитов достигала 28.9% в Ukreximbank и 23.7% в Oschadbank. Наибольшая рентабельность активов отмечена у Universal Bank – 3.1%, а уровень покрытия кредитных рисков резервами у PrivatBank и Credit Agricole Bank составил по 98%. Стандартизированные коэффициенты чувствительности между индексом корпоративной безопасности и ROA увеличиваются от 0,47 до 0,78, с CAR – от 0,33 до 0,66, тогда как для NPL сохраняется обратная связь от −0,52 до −0,70. Полученные результаты могут быть использованы регулирующими органами, руководством банковских учреждений и аналитическими организациями при разработке политики обеспечения финансовой безопасности в контексте структурной трансформации экономики.

КЛЮЧЕВЫЕ СЛОВА: финансовая экономика, финансовая устойчивость, банк, банковский сектор, банковская стабильность, кибербезопасность, Украина

КОНФЛИКТ ИНТЕРЕСОВ: авторы заявляют об отсутствии конфликта интересов

ФИНАНСИРОВАНИЕ: исследование не имело спонсорской поддержки (собственные ресурсы)

История статьи:
Получено 09 июля 2026
Принято 25 августа 2026
Опубликовано 30 сентября 2026

***Корреспондирующий автор: Полторак А.** – доктор наук, заведующая кафедрой менеджмента, бизнеса и администрации, Николаевский национальный аграрный университет, ул. Георгия Гонгадзе 9, 54008, Николаев, Украина, +380 512 709 331, email: anastasiiapoltorak7@gmail.com

INTRODUCTION

The stability of the banking sector has become a critical component of Ukraine's financial and economic security amid prolonged military uncertainty, structural disruptions, and rising systemic risks. The full-scale invasion has significantly changed the operating environment for Ukrainian banks, increasing the importance of adaptive management approaches to maintain solvency, operational continuity, and institutional resilience. Previous studies show that financial technologies, risk management mechanisms, and institutional adaptation help strengthen financial system stability under uncertainty (Sirenko et al., 2020; Poltorak et al., 2021). Recent research has also emphasised the importance of monitoring systems, digital transformation and external support mechanisms in maintaining financial stability during periods of crisis (Atamanyuk et al., 2024; Buriachenko et al., 2025).

Traditional approaches to banking management have mainly focused on individual financial indicators, including capital adequacy, liquidity, credit risks and profitability. However, the contemporary risk environment demonstrates that banking resilience depends not only on financial performance but also on a wider set of factors, including cybersecurity, information reliability, personnel stability, legal protection and reputational sustainability. Therefore, corporate security should be treated as an integrated management dimension that influences banks' ability to withstand systemic shocks and adapt to structural transformations.

This study addresses the insufficient integration of corporate security factors into comprehensive models for assessing and managing the financial stability of commercial banks under wartime conditions. Existing approaches often analyse separate risk categories or financial indicators without considering the interrelationship between different security components and their combined influence on banking resilience.

This study aims to assess the relationship between corporate security and the financial stability of Ukrainian banks and to develop a security-oriented management framework based on empirical assessment and post-war recovery scenarios. The study addresses the following research questions:

RQ1. What differences exist in the level of corporate security among Ukrainian commercial banks under wartime conditions?

RQ2. How is corporate security associated with key indicators of Ukrainian banks' financial stability?

RQ3. How can security-oriented management contribute to strengthening banking resilience under alternative post-war recovery scenarios?

The scientific novelty of the study lies in the development of an integrated framework for assessing corporate security as a multidimensional component of banking stability. Unlike approaches focused primarily on financial indicators, the proposed framework integrates financial, economic, informational, technological, personnel, legal, physical, and reputational dimensions and combines multidimensional assessment with scenario modelling to examine potential recovery trajectories of the Ukrainian banking sector. The practical contribution of the study lies in providing a structured analytical basis for identifying security vulnerabilities across banking institutions and supporting adaptive management decisions under conditions of macro-financial uncertainty.

LITERATURE REVIEW

Previous studies have examined banking stability from different perspectives, including financial security assessment, risk management, digital transformation and institutional resilience. Sirenko et al. (2020) showed that the development of financial technologies strengthens financial security by reducing shadow transactions and improving control over payment infrastructure. Poltorak et al. (2021) developed approaches for modelling financial security levels using multifactor systems of macroeconomic indicators, allowing the identification of stabilisation parameters within financial systems.

Recent research has expanded the understanding of banking resilience by incorporating monitoring mechanisms, technological development and organisational adaptation. Atamanyuk et al. (2024) proposed analytical monitoring approaches to identify systemic risks more quickly. Buriachenko et al. (2025) examined the influence of external economic, military and diplomatic factors on financial stability through exchange reserves, debt structures and financial markets.

Other studies have highlighted the importance of internal management mechanisms. Makarychev and Sazonov (2025) showed that weaknesses in institutional banking supervision may lead to reputational losses and reduced trust in financial institutions. Abidovna (2023) emphasised the importance of strengthening risk management units, integrating information technologies and improving human resource management practices. Siddique et al. (2022) demonstrated that loan portfolio quality and risk management approaches remain important determinants of banking performance.

Research conducted in different national contexts also highlights the importance of organisational flexibility, operational risk management and digital transformation. Al Zaidanin and Al Zaidanin (2021) examined the role of credit risk management in bank performance, while Hac et al. (2021) focused on risk management culture under changing macroeconomic conditions. Al-kiyumi et al. (2021) considered operational risk management, and Qasim and Anwar (2022) analysed credit risk management practices in commercial banks. More recently, Xie and Wang (2023) showed how digital transformation can affect the development and performance of commercial banks. Taken together, these studies indicate that banking resilience depends on both financial risk management and broader organisational and technological adaptation.

Against this background, security-oriented management can be considered a broader approach to banking resilience than traditional risk management. While traditional risk management primarily focuses on financial, credit, market and operational risks, security-oriented management also incorporates organisational, informational, technological, personnel, legal, reputational and physical dimensions. The main differences between these approaches are summarised in Table 1.

Table 1. Comparative characteristics of traditional risk management and security-oriented bank management

Criterion	Traditional risk management	Security-oriented bank management
Goal orientation	Minimisation of financial losses, compliance with regulations	Ensuring corporate resilience, protection against multi-vector threats, strategic stability
Objects of influence	Credit, market, operational and liquidity risks	All components of corporate security: financial, information, legal, personnel, technological, reputational
Time horizon	Short- and medium-term control of risk events	Long-term scenario planning and forecasting the impact of systemic threats
Management tools	Risk analysis, reserving, limiting, stress testing	Comprehensive compliance system, security audit, response protocols, cyber defense, adaptive strategies
Adaptability	Limited, mostly reactive	High, with elements of proactive management, dynamic updating of procedures

Note: compiled by the authors

Comparative analysis confirms that security-oriented management provides an expanded platform for banks' strategic responsibility under conditions of systemic instability and high uncertainty. Unlike traditional risk management, which is predominantly reactive and event-driven, a security-oriented approach encompasses a broader set of target parameters and integrates managerial, technological, and regulatory protection tools into a unified management architecture. It places particular emphasis on proactive monitoring, scenario forecasting, and preventive measures, which together form the foundation for long-term institutional stability in the context of post-war economic recovery.

Based on the reviewed literature and international regulatory approaches, corporate security in banking can be structured into eight interrelated components: financial, economic, information, physical, personnel, technological, reputational and legal security. These components and the indicators commonly used for their assessment are presented in Table 2.

Table 2. Matrix of components of corporate security of a banking institution and typical assessment indicators

Corporate security component	Typical indicators for evaluation
Financial security	Capital Adequacy Ratio (CAR), NPL ratio, liquidity, cost-to-income ratio, ROA, provisioning level
Information security	Number of cyber incidents, availability of a certified ISMS (ISO/IEC 27001), IT security costs, RTO, share of cybersecurity in the IT budget
Personnel security	Staff turnover, critical access share, integrity checks, labor violations
Technological security	Redundant data center, failure rate, digital readiness level, process automation
Legal security	Number of litigations, inspections with violations, regulatory compliance, legal risks
Reputational security	Trust index, negative mentions, customer satisfaction (CSAT), ratings (Moody's, S&P), scandals
Physical security	Physical intrusion incidents, security systems, evacuation training, access control
Economic security	Market share dynamics, currency dependence, client concentration, government regulation
CAR – Capital Adequacy Ratio; ROA – Return on Assets; NPL – Non-Performing Loans; ISMS – Information Security Management System; RTO – Recovery Time Objective; CSAT – Customer Satisfaction Score	

Note: authors' calculations based on National Bank of Ukraine (2025), Moody's Investors Service (2025), ISO/IEC (2022)

The components are closely interconnected. Weaknesses in information security may affect reputation, while personnel-related problems may increase legal and operational risks. A multidimensional assessment therefore provides a broader view of banking resilience than the analysis of individual financial indicators alone.

Despite the significant contribution of previous studies, several limitations remain. Existing research predominantly focuses either on financial indicators or on specific risk categories, such as credit risk, operational risk or cybersecurity. The institutional dimension of corporate security, including the combined influence of organisational, technological, informational and reputational factors on financial stability, remains insufficiently explored.

Therefore, this study addresses the research gap of a comprehensive model that integrates corporate security assessment with financial stability analysis and scenario-based forecasting for banks operating under wartime uncertainty. This study aims to address this gap by developing a multidimensional corporate security assessment framework and analysing its implications for the future resilience and recovery of the Ukrainian banking sector.

Despite the growing body of research on banking stability, most studies focus on individual financial indicators or specific types of risk, including credit, operational and cybersecurity risks. The broader concept of corporate security, which also includes organisational, technological, informational, personnel, legal, physical and reputational dimensions, has received less attention. There is also limited research combining such a multidimensional assessment with scenario analysis, particularly in the context of wartime uncertainty. This study addresses this gap by combining corporate security assessment with financial stability analysis and scenario analysis. The proposed framework is applied to Ukrainian banks to examine their resilience under wartime conditions and possible post-war recovery scenarios.

MATERIALS AND METHODS

The study employed an applied analytical and modelling approach to assess corporate security and financial stability in Ukrainian banks. The empirical assessment focused on 2024 as the reference year, while data for 2020–2023 were used, where relevant, to provide background information on changes in selected financial indicators and the broader transformation of the Ukrainian banking sector.

Primary statistical information was collected from the National Bank of Ukraine (2025) materials, specifically the Financial Stability section for 2020–2024. The analysis focused on ten banking institutions that, as of the end of 2024, held the largest market share in terms of assets, thereby ensuring representativeness of the sample and coverage of the key strategic players in the financial system. These included: Credit Agricole Bank (2025), Raiffeisen Bank International (2024), Universal Bank (2025), First Ukrainian International Bank

(2025), PrivatBank (2025), Ukrgasbank (2025), Oschadbank (2025), Ukreximbank (2025), A-Bank (2025) and OTP Bank (2025). The sample was selected based on the ranking of Ukrainian banks by total assets as of the end of 2024, according to National Bank of Ukraine statistics. The study included the ten largest banking institutions by asset volume, which collectively represented the major share of the Ukrainian banking sector and reflected different ownership models, including state-owned, foreign and private banks. The selection criterion was each bank's position in the asset ranking, while systemic importance, market coverage, and strategic role in the financial system were considered additional factors confirming the sample's representativeness. The analysis employed a stratification of banks by organisational type into three groups – state-owned, foreign and private – which enabled consideration of differences in strategic approaches to risk management depending on institutional status. Additionally, rating reports from international agencies, including S&P Global Ratings (Fojcik, 2024), Fitch Ratings (2024), and Moody's Investors Service (2025), were used to provide a comparative basis for assessing banking reliability under conditions of high macro-financial volatility.

The institutional basis of the security-oriented management framework drew on recommendations of the Basel Committee on Banking Supervision and the Bank for International Settlements (2022). International information-security standards were also considered, including ISO/IEC (2022) Information Security Management Systems – Requirements and NIST SP 800-53 issued by the National Institute of Standards and Technology (2020). These sources provided a regulatory and methodological basis for identifying the main dimensions of corporate security relevant to banks operating under wartime conditions and prospective post-war recovery.

Corporate security was assessed using a structural-functional approach. Eight components were distinguished: financial, economic, informational, physical, personnel, technological, reputational and legal security. Each component included a set of indicators derived from bank reporting, National Bank of Ukraine statistics and publicly available analytical sources.

The financial component included the capital adequacy ratio (CAR), non-performing loan ratio (NPL), return on assets (ROA) and provisioning coverage ratio. Economic security was assessed using indicators related to market position, client concentration and currency dependence. Information security covered information-security management, cybersecurity and operational reliability. The technological component reflected digital infrastructure, process automation and continuity of IT services. Personnel security included staff stability, personnel turnover and organisational resilience. Legal and reputational security covered regulatory compliance, legal risks, customer trust and reputation-related indicators. Physical security reflected the protection of critical infrastructure and operational continuity.

The indicators were normalised to the interval [0,1] using the min–max transformation. For stimulants, where higher values indicated stronger corporate security, the following formula was applied: $Zij=(Xij-Xmin)/(Xmax-Xmin)$. For destimulants, where higher values indicated increased risk, the reverse transformation was used: $Zij=(Xmax-Xij)/(Xmax-Xmin)$. Equal weights were assigned to all indicators within each component, and each of the eight components contributed equally to the final corporate security index. The integral corporate security index was calculated as the arithmetic mean of the eight component values.

An integral assessment was obtained by calculating the average value of normalised indicators within each block and aggregating the eight component scores with equal weights, which ensured comparability across banks and conceptualised corporate security as a multidimensional category. The average value was calculated according to the formula (1):

$$I_j = \frac{1}{n}\sum_{i=1}^{n} z_{ij} \quad (1)$$

where:

I_j – the integral indicator of block;

Zij – the normalised value of indicator;

n – the number of indicators in the respective block.

Banks were classified according to the value of the integral index. Values of 0.75 and above were interpreted as a high level of corporate security, values from 0.60 to below 0.75 as a medium level,

and values below 0.60 as a low level. The same thresholds were applied consistently across the analysed institutions.

Scenario analysis was used to examine banking stability under three alternative macro-financial conditions: protracted crisis, partial stabilisation and active recovery. The scenarios were characterised using five financial and risk parameters: NPL ratio, ROA, CAR, currency volatility and bank capitalisation. The scenario values were used as analytical assumptions for comparing possible changes in banking stability under different external conditions rather than as point forecasts of future outcomes.

To examine the relationship between corporate security and selected financial stability indicators, exploratory econometric analysis was conducted using simple ordinary least squares regression. Separate models were estimated for ROA, CAR, NPL, liquidity coverage and capitalization (2):

$$Y_i = \beta_0 + \beta_1 \times CS_i + \varepsilon_i \quad (2)$$

where:

Y_i – the selected financial stability indicator for bank;

CS_i – the integral corporate security index;

β_0 – the intercept;

β_1 – the estimated sensitivity coefficient, and ε_i is the error term;

ε_i – the error term.

Because several financial indicators used as dependent variables are also included in the financial component of the integral corporate security index, the regression coefficients were interpreted as exploratory sensitivity measures rather than independent causal effects. The purpose of the analysis was therefore to assess the direction and relative strength of associations between the overall security profile and selected financial stability parameters. The models were estimated using MS Excel and Python with the statsmodels package. Statistical significance was assessed at the 5% significance level ($p<0.05$). The results of the integral assessment and scenario analysis were subsequently used to identify differences in banks' security profiles and their sensitivity to alternative macro-financial conditions and to formulate a security-oriented management framework for wartime conditions and prospective post-war recovery.

RESULTS

The assessment of corporate security among Ukrainian commercial banks begins with a comparison of their main institutional and market characteristics. These characteristics provide the context for interpreting differences in corporate security across the selected institutions. Table 3 summarises the banks by ownership type, asset market share in 2024, regional presence and systemic importance.

Table 3. List of banks studied and their basic characteristics (2024)

Bank name	Property type	Asset market share, %	Regional presence	Systemic significance
JSC CB "PrivatBank"	State	20.1	All regions, the most extensive network	High
JSC "Oschadbank"	State	14	All regions, specialisation in state programs	High
JSC "Ukreximbank"	State	9.8	Central office, corporate network	High
JSC "Ukrgasbank"	State	5.7	100+ branches, green financing	Medium
JSC "Raiffeisen Bank"	Foreign	6.1	Present in 23 regions, digital channels	High
JSC "PUMB"	Private	4.2	Industrial regions, corporate segment	High
JSC "Universal Bank"	Private	4	Online model (Monobank), no branches	Medium
JSC "A-Bank"	Private	2.9	180+ branches, available in all regions	Medium
JSC "Credit Agricole Bank"	Foreign	2.5	Big cities, focus on the agricultural sector	Medium
JSC "OTP Bank"	Foreign	2.4	Emphasis on corporate lending	Medium

Note: authors' calculations based on the National Bank of Ukraine (2025), Credit Agricole Bank (2025), Raiffeisen Bank International (2024), Universal Bank (2025), First Ukrainian International Bank (2025), PrivatBank (2025), Ukrgasbank (2025), Oschadbank (2025), Ukreximbank (2025), A-Bank (2025), OTP Bank (2025), Fojcik (2024), Fitch Ratings (2024), Moody's Investors Service (2025)

The data presented in Table 3 show considerable structural differences among the selected banks in terms of ownership, asset market share and systemic importance. Four state-owned banks – PrivatBank (20.1%), Oschadbank (14.0%), Ukreximbank (9.8%) and Ukrgasbank (5.7%) – together account for 49.6% of the reported asset market share. This concentration highlights the important role of state-owned institutions in the Ukrainian banking system.

Foreign-owned banks, including Raiffeisen Bank (6.1%), Credit Agricole Bank (2.5%) and OTP Bank (2.4%), have smaller individual market shares but operate within international corporate governance and risk-management frameworks. Private banks, particularly PUMB (4.2%) and Universal Bank (4.0%), are characterised by business models with a strong focus on retail and digital services. These differences in ownership structure, market position and operating models provide an important context for the subsequent assessment of corporate security.

Differences in ownership, market scale, regional presence and operating models may be associated with different approaches to risk management and corporate security. These institutional characteristics are therefore considered when interpreting the financial and multidimensional security profiles of the analysed banks. The values of the selected financial indicators in 2024 show considerable variation across the analysed banks. Figure 1 presents capital adequacy, non-performing loans, return on assets and provisioning coverage, providing a basis for the comparative assessment of the financial component of corporate security.

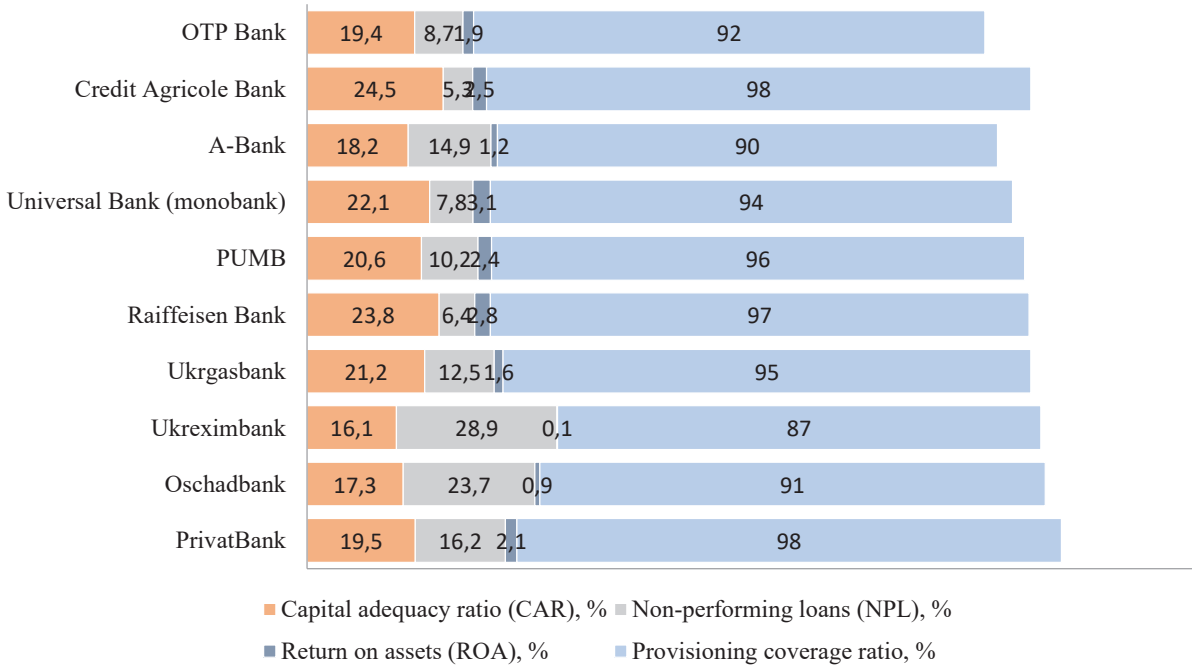


Figure 1. Selected financial indicators of Ukrainian banks, 2020-2024

The comparative analysis presented in Figure 1 shows considerable differences among Ukrainian banks in key financial security indicators. Credit Agricole Bank (24.5%) and Raiffeisen Bank (23.8%) recorded the highest capital adequacy ratios, indicating relatively strong capital buffers. By contrast, Ukreximbank showed the lowest value (16.1%), suggesting a lower capacity to absorb potential losses compared with the other banks in the sample. The share of non-performing loans exceeded 20% in Ukreximbank (28.9%) and Oschadbank (23.7%), indicating elevated credit risk. These institutions also recorded low or near-zero ROA values, which may limit their capacity to generate internal sources of capitalisation.

Universal Bank recorded the highest ROA (3.1%), indicating comparatively strong profitability. Loan loss provisioning was highest in PrivatBank and Credit Agricole Bank (98% each), suggesting a high level of coverage of identified credit risks. Overall,

the results show that the financial security profiles of the analysed banks differ substantially in terms of capital adequacy, asset quality, profitability and provisioning. However, financial indicators alone do not fully capture the multidimensional nature of corporate security. Figure 2 therefore extends the analysis by presenting the component structure of the integral corporate security index and identifying differences in banks' overall security profiles.

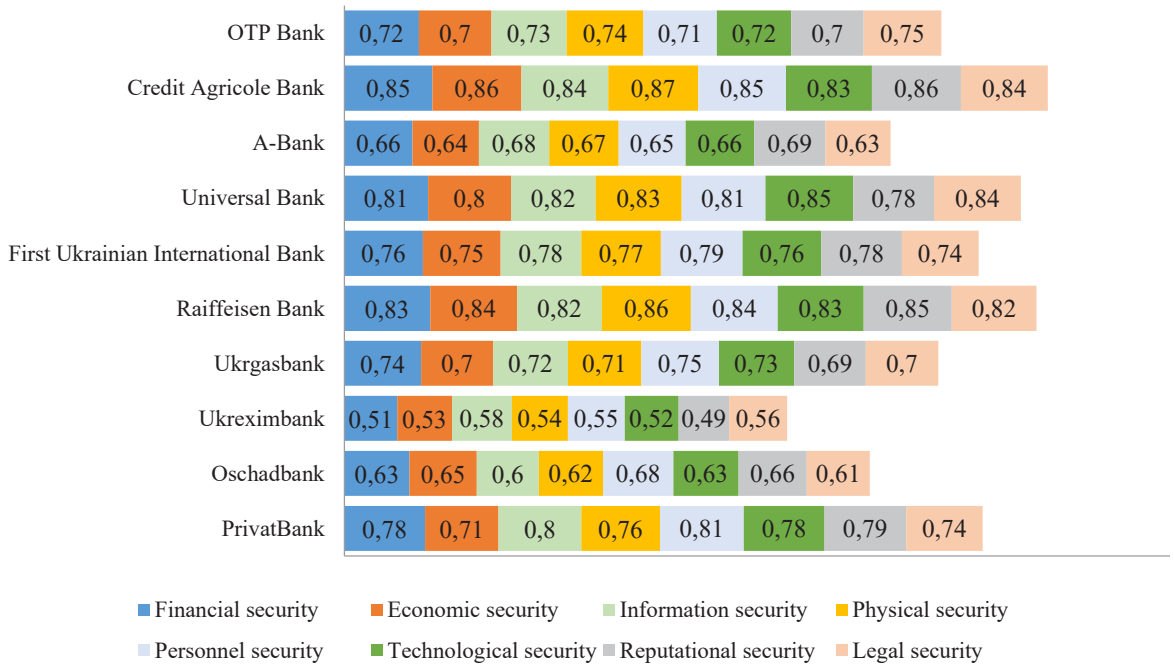


Figure 2. Integral assessment of the level of corporate security of Ukrainian banks by components, 2024

The final ranking of banks by integrated assessment of corporate security reveals a clear hierarchy of institutions by security level. The high-security group comprises Credit Agricole Bank (0.84), Raiffeisen Bank (0.85), Universal Bank (0.77), FUIB (0.75) and PrivatBank (0.76), all of which demonstrate a balanced profile across information, technological, financial and legal dimensions (with all indicators exceeding 0.70). The medium-security group includes Oschadbank (0.63), Ukrgasbank (0.71), A-Bank (0.64), and OTP Bank (0.70), where notable asymmetries are observed, particularly in the technological and economic components. Ukreximbank, with an integral score of 0.53, stands out as the only institution in the conditionally low-security category, mainly because of weak results in most components, especially reputation (0.49) and technology (0.52). These findings highlight both the strengths and vulnerabilities of individual banks' security systems.

The multidimensional assessment shows that corporate security cannot be explained by asset size or systemic importance alone. Differences are also associated with the balance of financial and non-financial security components, including information, technological, reputational and organisational dimensions. The results provide a basis for the subsequent scenario analysis and for identifying areas where individual banks may require greater managerial attention.

Based on the preceding assessment and the practices identified in regulatory, analytical and bank reporting sources, adaptive management measures were grouped into five functional areas. This classification links specific management practices with their expected contribution to banking resilience under conditions of heightened uncertainty. Table 4 summarises the proposed typology of adaptive management practices and their expected effects.

Table 4. Typology of adaptive management practices of banks by functional areas

Functional direction	Typical adaptive practices	Expected effect
Finances	Credit policy revision; accelerated provisioning; introduction of liquidity stress testing	Reducing credit risk; maintaining solvency; improving supervisory performance.
Human resources policy	Development of personnel reserve; remote personnel management; rotation and multifunctionality models	Stability of operational processes; reduction of losses due to staff turnover; increased management flexibility
Information technology	Transition to cloud infrastructure; implementation of zero trust architecture; institutionalization of SOC/CSIRT	Strengthening cyber resilience; protecting data and transactions; responding quickly to IT incidents
Legal environment	Centralisation of compliance procedures; integration of legal monitoring into operational activities	Reducing sanctions and reputational risks; increasing regulatory compliance.
Communications	Implementation of reputation intelligence tools; online monitoring of client signals; social risk management	Strengthening customer trust; timely response to image threats; increasing social capital

Note: authors' calculations based on the National Bank of Ukraine (2025), Credit Agricole Bank (2025), Raiffeisen Bank International (2024), Universal Bank (2025), First Ukrainian International Bank (2025), PrivatBank (2025), Ukrgasbank (2025), Oschadbank (2025), Ukreximbank (2025), A-Bank (2025), OTP Bank (2025), Fojcik (2024), Fitch Ratings (2024), Moody's Investors Service (2025)

The typology of adaptive management practices reflects banks' aspiration for a multi-vector transformation of their organizational models in a risk-prone environment. In the financial sphere, key measures include strengthening reserves and implementing liquidity stress testing, which respond to anti-crisis management requirements. The personnel dimension focuses on operational stability through the formation of multifunctional staff and the use of rotational mechanisms. Within the IT sector, approaches aimed at enhancing cyber resilience prevail, particularly through the adoption of zero-trust architecture and the activation of interaction with CSIRT units. The legal and communication blocks illustrate a shift towards integrated risk control, combining regulatory compliance with reputational transparency.

This framework forms the basis for the further development of a holistic model of security-oriented management, adapted to the post-war restoration of the financial system. The conceptual model of security-oriented management in banking institutions requires a clear definition of its structural components and the functional content of each block. To ensure the integrity of the management architecture, the model incorporates six key areas: risk management, cybersecurity, personnel, legal, reputational, and technological security. Each component operates autonomously yet remains interconnected in contributing to the bank's overall financial and economic stability. Table 5 presents a substantive description of these blocks, specifying their role in adaptive anti-crisis management.

Table 5. Components of the conceptual model of security-oriented management and their functional content

Model component	Functional purpose
Risk management	Identification, monitoring, and scenario forecasting of financial, operational, market, and geopolitical risks; construction of dynamic early warning indicator systems
Cybersecurity	Digital perimeter protection, anomalous activity monitoring, zero trust architecture implementation, and SOC/CSIRT institutionalization for rapid response
Personnel security	Formation of an adaptive personnel reserve, support for team stability, organization of internal training, ensuring management continuity in crises
Legal support	Ensuring legal compliance, prevention of sanctions and contractual risks, compliance monitoring, legal support for information protection

Reputational security	Monitoring social and public risks, image management in the digital environment, forecasting narrative threats, supporting the stability of trust.
Technological sustainability	IT infrastructure redundancy, scalability of digital services, ensuring functional continuity, implementation of adaptive architectures based on cloud technologies

Note: authors' calculations based on the Bank for International Settlements (2022), ISO/IEC (2022), National Institute of Standards and Technology (2020)

The proposed structural model offers a holistic perspective of the security management system as an interconnected complex of functional blocks. Particularly significant is the interaction between risk management and the technological and reputational subsystems, which enables the effective localisation of threats of both internal and external origin. Cybersecurity and legal support act as institutional filters, preventing critical incidents from escalating, while the human resource component underpins adaptability and continuity in management processes. The complexity of implementing each block is amplified by the integration of digital technologies, which, in the context of hybrid challenges, becomes a key determinant of banking stability. Accordingly, the model may serve as an analytical foundation for further deploying management transformation strategies aimed at strengthening systemic security.

It should be emphasised that modelling security-oriented management of commercial banks in the context of post-crisis recovery requires a multi-component approach, focused on the integration of functionally autonomous yet strategically interdependent management blocks. The proposed conceptual model encompasses six key areas – risk management, cybersecurity, human resources, legal, reputational, and technological security – which together form a holistic architecture for the stability of the banking system. Its adaptive character is grounded in verified empirical data and established anti-crisis practices, ensuring high relevance to contemporary challenges in a hybrid environment. This structural configuration provides the basis for developing institutional mechanisms to enhance financial stability, a defining element of the state's broader system of financial and economic security.

To assess the economic potential of a security-oriented management model for banking institutions, modeling scenarios for the development of the macro-financial environment is particularly important. Given the complex security situation and the multi-vector nature of external risks, it is appropriate to distinguish three basic contexts of banking sector functioning: protracted crisis, partial stabilisation, and active economic recovery. Each scenario corresponds to a specific risk profile that determines banks' susceptibility to macroeconomic shocks and the variability of financial outcomes, depending on the depth of integration of security practices. A comparative analysis of these conditions makes it possible to identify the stabilising effect of corporate security measures and to assess the potential efficiency gains from their systemic implementation. Table 6 presents the key parameters used to characterise three alternative macro-financial scenarios.

Table 6. Key parameters of alternative macro-financial scenarios

Risk parameter	Scenario 1: Protracted crisis	Scenario 2: Partial stabilisation	Scenario 3: Active recovery
NPL, %	22.0-26.5	13.0-14.5	7.0-8.5
ROA, %	0.3-0.6	1.2-1.5	3.0-3.4
CAR, %	15.0-17.0	19.0-21.0	22.5-24.0
Currency volatility (UAH/USD)	High (>20% fluctuation)	Moderate (8-12%)	Low (<5%)
Annual bank capitalisation growth, %	Negative/close to zero	Stable growth (5-7%)	Accelerated growth (10-13%)

Note: authors' calculations based on the National Bank of Ukraine (2025), Fojcik (2024), Fitch Ratings (2024), Moody's Investors Service (2025)

The scenario approach provides a structured basis for examining how key financial stability indicators may vary under different macro-financial conditions. The three scenarios are differentiated by the expected levels of NPLs, ROA, CAR, currency volatility and bank capitalisation. These parameters allow the financial risk environment to be compared across conditions ranging from prolonged instability to active recovery.

In the protracted crisis scenario, systemic instability reaches critical levels. This is reflected in persistently high NPLs and a sharp decline in ROA to 0.3-0.6p.p., signaling minimal profitability of banking operations. CAR falls to 15.0-17.0 p.p., indicating capital erosion, while currency volatility exceeds 20 p.p., amplifying solvency risks. Capitalisation rates either stagnate or turn negative, which threatens investor withdrawals and necessitates regulatory intervention. Without integrated security mechanisms, these dynamics may have a cumulative destabilizing effect, exacerbating banks' vulnerability to multiple risk factors.

The partial stabilisation scenario reflects moderate improvements in financial security. NPLs decline to 13.0-14.5 p.p., indicating gradual rehabilitation of loan portfolios. ROA stabilises at 1.2-1.5p.p., while CAR returns to controlled levels of 19.0-21.0 p.p., providing sufficient capital to sustain ongoing operations. Currency volatility falls to 8-12%, and annual capitalisation rates reach 5-7%, signalling a revival of investor confidence. Implementing security-oriented management models can reinforce these trends by improving flexibility in risk management, compliance systems, and human resource adaptation.

The active recovery scenario demonstrates the most favourable conditions for financial security. NPLs are reduced to 7.0-8.5p.p., and ROA rises to 3.0-3.4p.p., indicating effective use of the resource base. CAR increases to 22.5-24.0p.p., ensuring a strong capacity to absorb risks and support credit expansion. Currency fluctuations fall to below 5%, evidencing monetary market stabilisation, while capitalisation accelerates to 10-13% annually. This scenario provides the most conducive environment for the large-scale implementation of security-oriented management practices, ensuring systemic resilience through the integration of cybersecurity, anti-crisis human resource strategies, reputation monitoring and legal predictability.

To complement the scenario analysis, regression modelling was used to examine the direction and relative strength of the association between the corporate security index and selected financial stability indicators. Standardised coefficients were estimated under the three scenario settings to compare the sensitivity of financial indicators under conditions of prolonged crisis, partial stabilisation and active recovery. The resulting coefficients are interpreted as exploratory sensitivity measures rather than causal effects and are presented in Table 7.

Table 7. Standardised sensitivity coefficients between corporate security and financial stability indicators under alternative scenarios

Financial indicator	Scenario 1: Protracted crisis	Scenario 2: Partial stabilisation	Scenario 3: Active recovery
ROA	+0.47	+0.62	+0.78
CAR	+0.33	+0.51	+0.66
NPL	-0.52	-0.61	-0.70
Capitalisation growth	+0.28	+0.49	+0.67
Liquidity	+0.39	+0.54	+0.72

Note: authors' calculations based on the National Bank of Ukraine (2025), Fojcik (2024), Fitch Ratings (2024)

The modeling results show that banks' financial indicators are highly sensitive to changes in the integral level of corporate security across all scenarios. In particular, the increase in ROA, with a coefficient of +0.78 in the active recovery scenario, shows that higher levels of corporate security are associated with higher profitability indicators. Similarly, CAR and capitalisation rates show significant positive dynamics with rising levels of corporate security, reflecting the strengthening of banks' resource base and their capacity for autonomous financing. The negative correlation with NPL confirms the effectiveness of corporate control mechanisms in reducing credit risks. Liquidity proved to be the most dynamic parameter: under conditions of high corporate security, it increased

most substantially, indicating banks' adaptive capacity to maintain solvency even under stress.

The combined results of scenario and econometric modeling confirm that the introduction of a security-oriented management model generates considerable effects not only at the level of individual institutions, but also at the macro-financial level. The established regression relationships demonstrate the statistical association between the corporate security profile and key financial stability parameters of banks – profitability, asset quality, capitalization and liquidity – with the strength of these effects increasing under conditions of economic growth. Policymakers can incorporate these interdependencies into banking regulatory policy, particularly when designing indicative mechanisms for assessing financial stability. The findings thus reaffirm the role of corporate security as a critical component of financial architecture during structural transformation and post-war economic recovery.

DISCUSSION

The results of the analysis revealed significant interbank differentiation in the level of corporate security, which stemmed from differences in organisational structure, ownership type, risk management practices, and the depth of digital transformation. The analysis showed that institutions with high integral security index values also demonstrated stable key financial indicators and reduced sensitivity to external destabilizing factors, as confirmed by scenario modeling. The identified correlation between the balance of functional security blocks and institutions' adaptability to changes in the macro-financial environment validated the application of the multidimensional assessment model.

The developed typology enabled the stratification of banking institutions by the level of comprehensive security, thereby identifying systemic areas of vulnerability and creating an empirical basis for constructing adaptive scenarios in the banking sector. A multidimensional model of corporate security, encompassing key risk management blocks, proved effective under conditions of macro-financial instability. Zan (2024) proposed a similar approach, highlighting the importance of integrating internal management mechanisms with external regulatory factors. His work underscores the need for consistency between institutional processes and preventive monitoring of systemic risks as prerequisites for financial stability. The correlation of results confirmed the feasibility of implementing such a model in banking security management.

The stratified analysis further showed that the effectiveness of risk management depends not only on asset size or ownership form, but also on institutions' capacity to adapt amid external turbulence. Kacicka (2023) also addressed strategic flexibility in management decisions, using the food industry as an example to examine the possibility of combining strategic planning with innovative risk management. The findings confirmed the universality of this approach for sectors highly sensitive to environmental changes, including the banking system. The study found that the ability to restructure management processes rapidly plays a decisive role in enhancing overall institutional security.

As part of the study of systemic threats, it was established that traditional regulatory tools do not adequately respond to multi-vector risks. The findings of Ellis et al. (2022) confirmed the need to improve methods of measuring systemic risks, considering transformational dynamics of the financial environment. Their work emphasises that the transition to a comprehensive measurement of cross-functional risks is critical for modern regulatory practice. The results of this study provided an empirical basis for developing such tools, highlighting the need to expand traditional risk assessment methodology.

The theoretical framework set out by Schweizer (2019) formed the foundation for a deeper understanding of systemic threats as phenomena of complex adaptive systems. Within the scope of this research, such an approach allowed for a reorientation of the analytical focus from the analysis of individual financial indicators to their interaction with the structural parameters of corporate governance. Including personnel, information, and legal security enabled the construction of a holistic model of multi-component security for banking institutions. This ensured the integration of qualitative and quantitative variables in developing the integral corporate security index.

The structural-functional approach used in the study aligns with the concept presented by Bacciu et al. (2022), which demonstrated the need for systemic

risk management that incorporates interdisciplinary determinants. In their work, fire risk modeling was carried out; however, this study adapted the approach to the banking sector by interpreting the cumulative effects of security breaches. This adaptation made it possible to consider both the physical component and the informational and cyber aspects of institutional functioning, which is particularly important amid post-crisis economic turbulence.

The analysis of digital factors for enhancing management efficiency revealed that the digital transformation of banking processes positively influences the operational contour of corporate security systems. These findings align with the case study by Bueno et al. (2024), which examined digitalization as a tool for strengthening risk management and internal control. The study found that banks with a high level of digital integration had lower transaction costs, more efficient data-processing procedures, and greater adaptability to external challenges.

Scenario modeling results also showed that digital infrastructure is a key factor in shaping banks' institutional resilience to macro-financial and regulatory shocks. A similar relationship between technological adaptation and vulnerability reduction was identified by Zaman et al. (2023) in the context of logistics chains in the e-commerce sector. In the banking sector, analogous mechanisms were observed in the assessment of organisational flexibility, which ensured the continuity and stability of processes even under intensifying external risks. The decisive role of digital tools in this process makes the technological component an integral element of the architecture of multidimensional corporate security.

The analysis also examined how artificial intelligence (AI) tools improve the efficiency of information and cybersecurity systems. According to the framework proposed by Rodrigues et al. (2022), a cognitive model of interaction between AI, digital transformation, and cybersecurity strengthens the integration of technological solutions into the protective infrastructure of financial institutions. Within the present study, this approach was adapted to the corporate security model by incorporating the level of information security as one of its functional components.

In examining operational efficiency, a positive correlation was recorded between the degree of digital transformation and indicators of financial inclusion. The findings of Mavlutova et al. (2023) confirm that the expansion of digital services enhances the accessibility of banking services, which in turn contributes to the resilience and stability of the financial system. Consistent with this, the present study established that institutions with more advanced digital infrastructures demonstrated higher levels of operational efficiency, thereby reducing their vulnerability to financial risks.

The importance of information security as a determinant of user trust in banking services was reinforced by the study of Zhang et al. (2023), which found that the level of cybersecurity significantly influences customers' willingness to adopt fintech solutions. The analysis of corporate security indicators within this research similarly revealed a positive relationship between the level of information security and the composite resilience index, corroborating earlier scientific findings.

The type of bank influences how security management models are implemented. In particular, Raouf and Ahmed (2022) demonstrated that the effectiveness of risk management systems varies considerably between traditional and Islamic banks in the GCC countries. They concluded that the clear regulation of internal control procedures, inherent in specialised institutional structures, has a positive impact on institutional stability. The present study observed a similar trend, where banks with formalized internal audit policies showed greater resilience.

The analysis of information support for management processes showed that effective digital management accounting systems enhance transparency and reduce operational risks. Oudat (2021) substantiated the relationship between the quality of information systems and banking stability. The criteria applied in this study confirmed higher levels of information security in banks that had introduced modern analytical platforms and automated compliance mechanisms.

Intellectual capital and human resource policy were also identified as key components of corporate security. Ullah et al. (2021) found that the existence of a developed knowledge management system and structured staff training is positively correlated with financial stability. The present analysis confirmed similar relationships: banks with higher human resource security scores showed stronger adaptability

under risk scenarios, underscoring the importance of human capital in security management strategies.

The legal component – encompassing regulatory compliance and digital compliance control – was likewise recognised as a critical dimension of banking security. Chao et al. (2022) proposed a taxonomy of RegTech tools for monitoring financial stability, with particular emphasis on automated risk detection and adherence to regulatory standards. This study adopted a comparable approach, evaluating legal metrics as a distinct block of the corporate security model. This enabled the identification of a direct link between the degree of regulatory control and institutional resilience to supervisory challenges. Integrating digital compliance tools into risk management frameworks provided an additional protective layer against systemic regulatory failures.

In the economic security block, the study found that financial diversification is a significant factor in the stability of banking institutions in a changing environment. Xie et al. (2022) substantiated the importance of income diversification strategies as a means of enhancing financial stability. The results confirmed the hypothesis: banks with a broad product portfolio and a diversified client base showed higher levels of economic and financial security. Such diversification enabled greater flexibility of financial policy and a more effective response to external crises.

Financial forecasting was identified as one of the key tools of strategic planning under conditions of macro-financial instability. Kumar (2023) showed that multifactor forecasting models significantly influence the quality of management decisions in the financial sector. In this study, a scenario-based approach to assessing the integral corporate security index was implemented, enabling identification of potential risk configurations and evaluation of banking institutions' resilience to changes in the external environment. This model provided the foundation for developing preventive strategies for financial adaptation.

Digital automation tools, analysed by Singireddy et al. (2024), were assessed as critically important for transforming banks' management practices. The authors highlighted the role of smart automation, secure access systems and predictive intelligence in optimising risk management processes. The results confirmed that institutions with higher digital integration achieved stronger technological and information security, which contributed to enhanced overall corporate resilience. Adopting these technologies ensured consistent management decisions and minimized the influence of the human factor.

In the context of global economic transformations, uncertainty management as a strategic balancing tool has become particularly important. Iriani et al. (2024) emphasised the need to integrate qualitative analyses of the external environment with quantitative methods in order to improve the accuracy of strategic decisions. In this study, this concept was operationalized through a multi-level security assessment model, enabling risk evaluation at the intersection of functional blocks. This approach supported the development of an adaptive corporate governance system relevant to the conditions of a transformational economy.

Modern research has devoted considerable attention to the role of digital tools in strengthening the financial stability of banking institutions. Challa et al. (2024) examined the impact of technological solutions on investment stability and the reduction of transaction risks. The authors proposed a multi-level model combining cybersecurity platforms, automated monitoring protocols and elements of predictive analysis. This concept aligns with the conclusions of the present study, which recorded high values of information and technological security in banks with a developed digital architecture.

In the context of intelligent risk management, this study analyzed Vyas's (2025) approach, emphasizing the use of AI to develop cognitive threat management systems. The model integrated adaptive self-learning algorithms designed to improve decision-making accuracy in financial forecasting. The findings confirmed the need to develop a multi-vector security system that reflects the multifactorial nature of risks during the post-crisis reconfiguration of the banking system. This approach provided an empirical basis for assessing the effectiveness of intelligent elements in institutions' strategic adaptation.

The research confirmed the feasibility of using a security-oriented management model as a holistic response to threats from structural shifts in the macro-financial environment. The integral corporate security index, developed from eight functional blocks, revealed internal differentiation among banks based on digital transformation, strategic

flexibility, and financial resilience. The analysis identified areas of heightened risk and demonstrated structural heterogeneity in approaches to security management. The applied stratified assessment methodology proved effective in comparing institutions with varying levels of technological maturity.

The correlation between the results and findings from digital transformation, intelligent risk management, RegTech, and strategic financial forecasting underscores the relevance of the chosen approach. This interdisciplinary consistency highlights the need to improve further banking management models aimed at preventing systemic risks in unstable environments. Such models should integrate quantitative analysis, technological diagnostics, and scenario simulations, thereby ensuring the flexibility and adaptability of the banking sector under conditions of macro-financial transformation.

CONCLUSIONS

As part of the study, a methodological model for stratifying banking institutions by the level of corporate security was developed and tested, based on the construction of an integral index comprising eight functional blocks: financial, information, economic, physical, personnel, technological, reputational and legal security. On the basis of the obtained values of the integral indicator, the ten largest banks of Ukraine were stratified. The assessment showed significant differences among Ukrainian banks in corporate security levels. Institutions with higher integrated security profiles showed more balanced performance across functional components, whereas lower-security institutions demonstrated greater internal disparities requiring targeted managerial improvement. The identified asymmetries between individual security components indicated internal imbalances in management practices related to integrating security functions.

Scenario modeling produced three alternative trajectories of macro-financial development: a protracted crisis, partial stabilization, and active reconstruction. For each scenario, the levels of problem debt, asset profitability, capital adequacy, currency volatility and capitalisation were determined. Scenario modeling showed that strengthening corporate security is associated with improved financial stability, including reduced credit risk, higher profitability potential, and greater resilience under favorable recovery conditions. This dependence confirmed the strategic importance of strengthening functional security mechanisms for enhancing the financial stability of banking institutions.

The study has certain limitations. It is limited to a sample of only the ten largest banks, lacks complete data to assess some components of corporate security, relies on estimation assumptions in scenario modeling, and is affected by changes in the regulatory environment that affect the relevance of certain indicators. Further research should therefore expand the sample to include medium- and small-scale institutions, as well as adapt the model for regional and international comparative analysis. Another important direction is to integrate regulatory supervision indicators and explore relationships between digital transformation, the level of compliance control, and scenario adaptability. Applying machine learning methods to build predictive corporate security models that account for dynamic interactions among functional blocks in a changing financial environment also appears promising.

AUTHOR CONTRIBUTIONS

Conceptualization and theory: HF; research design: AP, HF, OB, AS and AA; data collection: OB; analysis and interpretation: AS and AA; writing draft preparation: AP, HF, OB, AS and AA; supervision: AP; correction of article: AP, HF, OB, AS and AA; proofread and final approval of article: AP, HF and AA. All authors have read and agreed to the published version of the manuscript.

REFERENCES

A-Bank. (2025). Information for shareholders and stakeholders. Retrieved April 30, 2026 from https://a-bank.com.ua/about/for-stakeholders

Abidovna, A.S. (2023). Modern trends in management strategies and their application in commercial banks. *Gospodarka i Innowacje*, *41,* 326-332.

Al Zaidanin, J.S., Al Zaidanin, O.J. 2021. The impact of credit risk management on the financial performance of United Arab Emirates commercial banks. *International Journal of Research in Business and Social Science*, *10*(3), 303-319. https://doi.org/10.20525/ijrbs.v10i3.1102

AL-kiyumi, R.K., AL-hattali, Z.N., & Ahmed, E.R. (2021). Operational risk management and customer

complaints in Omani banks. *Journal of Governance and Integrity*, *5*(1), 200-210. https://doi.org/10.15282/jgi.5.1.2021.7031

Atamanyuk, I., Poltorak, A., Sidenko, I., Bartnicka, E., & Kondratenko, Y. (2024). Concept of express monitoring of the state's financial security. *Proceedings of the 22nd Industrial Simulation Conference (ISC 2024)*, 24–29.

Bacciu, V., Sirca, C., & Spano, D. (2022). Towards a systemic approach to fire risk management. *Environmental Science & Policy*, *129,* 37-44. https://doi.org/10.1016/j.envsci.2021.12.015

Bank for International Settlements. (2022). Principles for Operational Resilience. Retrieved April 30, 2026 from https://www.bis.org/fsi/fsisummaries/op_resilience.htm.

Bueno, L.A., Sigahi, T.F., Rampasso, I.S., Leal Filho, W., & Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. *International Journal of Information Management Data Insights*, *4*(1), 100230. https://doi.org/10.1016/j.jjimei.2024.100230.

Buriachenko, O., Somak, O., Golubytskyi, S., Kravchenko, N., & Kravchenko, O. (2025). International support for Ukraine: Evaluating the impact of military, economic, and diplomatic aid. *Revista de Cercetare si Interventie Sociala*, *88*, 151-168.

Challa, S.R., Challa, K., Lakkarasu, P., Sriram, H.K., & Adusupalli, B. (2024). Strategic financial growth: Strengthening investment management, secure transactions, and risk protection in the digital era. *Journal of Artificial Intelligence and Big Data Disciplines*, *1*(1), 97-108. https://doi.org/10.70179/1kfdwj89

Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. *International Review of Financial Analysis*, *80*, 102023. https://doi.org/10.1016/j.irfa.2022.102023.

Credit Agricole Bank. (2025). Fourth quarter and full year 2024 results. Retrieved April 30, 2026 from https://www.credit-agricole.com/en/finance/financial-results/fourth-quarter-and-full-year-2024-results.

Ellis, S., Sharma, S., & Brzeszczyński, J. 2022. Systemic risk measures and regulatory challenges. *Journal of Financial Stability*, *61,* 100960. https://doi.org/10.1016/j.jfs.2021.100960.

First Ukrainian International Bank. (2025). Annual reports. Retrieved April 30, 2026 from https://about.pumb.ua/en/finance/annual_reports.

Fitch Ratings. (2024). Fitch Upgrades 7 Ukrainian Banks' IDRs on Sovereign Rating Action. Retrieved April 30, 2026 from https://www.fitchratings.com/research/banks/fitch-upgrades-7-ukrainian-banks-idrs-on-sovereign-rating-action-23-09-2024.

Fojcik, B. 2024. Ukrainian banks tested by tax hike, capital changes. Retrieved April 30, 2026 from https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/12/ukrainian-banks-tested-by-tax-hike-capital-changes-86653459.

Hac, L.D., Dinh, H.T., Nguyen, T.N., Bui, C.M., Phạm, N.T., Tran, T.D., & Tran, A.T. (2021). Enhancing risk management culture for sustainable growth of Asia commercial bank -ACB in Vietnam under mixed effects of macro factors. *Entrepreneurship and Sustainability Issues,* *8*(3), 291-307. http://doi.org/10.9770/jesi.2021.8.3(18).

Iriani, N., Agustianti, A., Sucianti, R., Rahman, A., Putera, W. 2024. Understanding risk and uncertainty management: A qualitative inquiry into developing business strategies amidst global economic shifts, government policies, and market volatility. *Golden Ratio of Finance Management*, *4*(2), 62-77. https://doi.org/10.52970/grfm.v4i2.444.

ISO/IEC (2022). Information security, cybersecurity and privacy protection — Information security management systems – Requirements. Retrieved April 30, 2026 from https://www.iso.org/standard/27001.

Kacicka, G. (2023). Adaptive risk management in food industry enterprises: Integration of strategies and innovations in an environment of economic instability. *International Interdisciplinary Scientific Journal" Expert"*, *1*(1), 73-88. https://doi.org/10.62034/2815-5300/2023-v1-i1-006

Kumar, R. 2023. The role of financial forecasting in corporate decision-making and strategic planning. *International Journal of Exploring Emerging Trends in Engineering*, *10*(2), 530-542. https://ijoeete.com/wp-content/uploads/2025/01/76-rajesh-kumar.pdf

Makarychev, A., & Sazonov, V. (2025). Governmentality, financial security and money laundering: the Estonian case of Danske Bank. *Security Journal*, *38*(1), 16. https://doi.org/10.1057/s41284-025-00463-7

Mavlutova, I., Spilbergs, A., Verdenhofs, A., Natrins, A., Arefjevs, I., Volkova, T. 2022. Digital transformation as a driver of the financial sector sustainable development: An impact on financial inclusion and operational efficiency. *Sustainability*, *15*(1), 207. https://doi.org/10.3390/su15010207

Moody's Investors Service. (2025). Financial Institutions – Ukraine. Retrieved April 30, 2026 from https://www.moodys.com/researchandratings/region/europe/ukraine/04208C/005001

National Bank of Ukraine. (2025). *Financial Stability Reports and Indicators*. Retrieved April 30, 2026 from https://bank.gov.ua/ua/stability

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations. Retrieved April 30, 2026 from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Oschadbank. (2025). Financial reporting. Retrieved April 30, 2026 from https://www.oschadbank.ua/en/finansova-zvitnist

OTP Bank. (2025). Bank reporting. Retrieved April 30, 2026 from https://www.otpbank.com.ua/about/informations/annual-reports/

Oudat, M. (2021). Accounting information system and financial sustainability of commercial and Islamic banks: A review of the literature. *Journal of Management Information and Decision Sciences*, *24*(5). https://doi.org/10.2139/ssrn.5147108

Poltorak, A., Potryvaieva, N., Kuzoma, V., Volosyuk, Y., & Bobrovska, N. (2021). Development of doctrinal model for state financial security management and forecasting its level. *Eastern-European Journal of Enterprise Technologies*, *5*(13), 26-33. https://doi.org/10.15587/1729-4061.2021.243056.

PrivatBank. (2025) Financial statements. Retrieved April 30, 2026 from https://privatbank.ua/about/finansovaja-otchetnost.

Qasim, S.S., & Anwar, M.M. (2022). Analyzing credit risk management in commercial banks: An exploratory research about the opinions of a sample of managers and heads of departments in selected commercial banks in Erbil City (2021). *Iraq Journal for Economic Sciences*, 20(73), 105–125. https://doi.org/10.31272/IJES2022.73.7

Raiffeisen Bank International. (2024). Annual Report. Retrieved April 30, 2026 from https://www.rbinternational.com/content/dam/rbi/ho/investors/results-reports/annual-reports/rbi/2025-02-25%202024%20RBI%20Annual%20Report.pdf.coredownload.pdf.

Raouf, H., Ahmed, H. 2022. Risk governance and financial stability: A comparative study of conventional and Islamic banks in the GCC. *Global Finance Journal*, *52*, 100599. https://doi.org/10.1016/j.gfj.2020.100599.

Rodrigues, A.R., Ferreira, F.A., Teixeira, F.J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, *60,* 101616. https://doi.org/10.1016/j.ribaf.2022.101616.

Schweizer, P.J. (2019). Systemic risks-concepts and challenges for risk governance. *Journal of Risk Research*, *24*(1), 78-93. https://doi.org/10.1080/13669877.2019.1687574.

Siddique, A., Khan, M.A., Khan, Z. (2022). The effect of credit risk management and bank-specific factors on the financial performance of the South Asian commercial banks. *Asian Journal of Accounting Research*, *7*(2), 182-194. https://doi.org/10.1108/AJAR-08-2020-0071

Singireddy, S., Adusupalli, B., Pamisetty, A., Mashetty, S., Kaulwar, P.K. (2024). Redefining financial risk strategies: The integration of smart automation, secure access systems, and predictive intelligence in insurance, lending, and asset management. *Journal of Artificial Intelligence and Big Data Disciplines*, *1*(1), 109-124. https://doi.org/10.70179/k86dcv60.

Sirenko, N., Atamanyuk, I., Volosyuk, Y., Poltorak, A., Melnyk, O., Fenenko, P. 2020. Paradigm changes that strengthen the financial security of the state through FINTECH development. In *Proceedings of the 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 110-116). Kyiv: IEEE. https://doi.org/10.1109/DESSERT50317.2020.9125026.

Ukreximbank. (2025) IFRS financial statements. Retrieved April 30, 2026 from https://www.eximb.com/eng/menu/profile-ukreximbank/financial-statements/ifrs-financials.html.

Ukrgasbank. (2025). Auditor's report and financial results. Retrieved April 30, 2026 from https://www.ukrgasbank.com/en/about/fin_results/auditors_report/.

Ullah, A., Pinglu, C., Ullah, S., Qian, N., Zaman, M. 2021. Impact of intellectual capital efficiency on financial stability in banks: Insights from an emerging economy. *International Journal of Finance & Economics*, 28(2), 1858-1871. https://doi.org/10.1002/ijfe.2512.

Universal Bank. (2025) Financial reports. Retrieved April 30, 2026 from https://www.universalbank.com.ua/financial-reports.

Vyas, A. (2025). Revolutionizing risk: The role of artificial intelligence in financial risk management, forecasting, and global implementation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5224657.

Xie, X., & Wang, S. (2023). Digital transformation of commercial banks in China: Measurement, progress and impact. *China Economic Quarterly International*, *3*(1), 35-45. https://doi.org/10.1016/j.ceqi.2023.03.002.

Xie, Z., Liu, X., Najam, H., Fu, Q., Abbas, J., Comite, U., Cismas, L.M., & Miculescu, A. (2022). Achieving financial sustainability through revenue diversification: A green pathway for financial institutions in Asia. *Sustainability*, *14*(6), 3512. https://doi.org/10.3390/su14063512.

Zaman, S.I., Khan, S.A., Qabool, S., & Gupta, H. (2023). How digitalization in banking improve service supply chain resilience of e-commerce sector? A technological adoption model approach. *Operations Management Research*, *16*(2), 904-930. https://doi.org/10.1007/s12063-022-00341-0.

Zan, W. (2024). Integrated strategies in risk management and financial stability. In: *Proceedings of the 2nd International Conference on Management Innovation and Economy Development (MIED 2024)* (pp. 559-565). London: Atlantis Press. https://doi.org/10.2991/978-94-6463-542-3_64.

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M.F., & Li, Z. (2023). Data security, customer trust and intention for adoption of Fintech services: An empirical analysis

from commercial bank users in Pakistan. *Sage Open*, *13*(3). https://doi.org/10.1177/21582440231181388.

Zhu, C., Zhu, N., Emrouznejad, A., & Ye, T. (2024). A new Malmquist productivity index with an application to commercial banks. *IMA Journal of Management Mathematics*, *35*(2), 215-240. https://doi.org/10.1093/imaman/dpad015.

Information about the authors

***Anastasiia Poltorak** – Full Doctor, Head of the Department of Management, Business and Administration, Mykolaiv National Agrarian University, Mykolaiv, Ukraine, email: anastasiiapoltorak7@gmail.com, ORCID ID: https://orcid.org/0009-0008-9620-4425

Hanna Fedosieieva – Full Doctor, Associate Professor, Department of Management, Business and Administration, Mykolaiv National Agrarian University, Mykolaiv, Ukraine, email: h.fedosieieva@outlook.com, ORCID ID: https://orcid.org/0009-0009-3536-0173

Olena Bodnar – PhD, Associate Professor, Department of Finance, Banking and Insurance, Mykolaiv National Agrarian University, Mykolaiv, Ukraine, email: o-bodnar@hotmail.com, ORCID ID: https://orcid.org/0009-0006-3099-3076

Anna Sukhorukova – PhD, Associate Professor, Department of Management, Business and Administration, Mykolaiv National Agrarian University, Mykolaiv, Ukraine, email: asukhorukova@outlook.com, ORCID ID: https://orcid.org/0009-0002-2550-1218

Andrii Ahafonov – Postgraduate Student, Mykolaiv National Agrarian University, Mykolaiv, Ukraine, email: aahafonov@hotmail.com, ORCID ID: https://orcid.org/0009-0005-8651-8197

Авторлар туралы мәліметтер

***Полторак А.** – ғылым докторы, менеджмент, бизнес және әкімшілік кафедрасының меңгерушісі, Николаев ұлттық аграрлық университеті, Николаев, Украина, email: anastasiiapoltorak7@gmail.com, ORCID ID: https://orcid.org/0009-0008-9620-4425

Федосеева А. – ғылым докторы, доцент, менеджмент, бизнес және әкімшілік кафедрасы, Николаев ұлттық аграрлық университеті, Николаев, Украина, e-mail: h.fedosieieva@outlook.com, ORCID ID: https://orcid.org/0009-0009-3536-0173

Боднар Е. – ғылым кандидаты, доцент, қаржы, банк ісі және сақтандыру кафедрасы, Николаев ұлттық аграрлық университеті, Николаев, Украина, e-mail: o-bodnar@hotmail.com, ORCID ID: https://orcid.org/0009-0006-3099-3076

Сухорукова А. – PhD, доцент, менеджмент, бизнес және әкімшілік кафедрасы, Николаев ұлттық аграрлық университеті, Николаев, Украина, email: asukhorukova@outlook.com, ORCID ID: https://orcid.org/0009-0002-2550-1218

Агафонов А. – аспирант, Николаев ұлттық аграрлық университеті, Николаев, Украина, email: aahafonov@hotmail.com, ORCID ID: https://orcid.org/0009-0005-8651-8197

Сведения об авторах

***Полторак А.** – доктор наук, заведующая кафедрой менеджмента, бизнеса и администрации, Николаевский национальный аграрный университет, Николаев, Украина, email: anastasiiapoltorak7@ gmail.com, ORCID ID: https://orcid.org/0009-0008-9620-4425

Федосеева А. – доктор наук, доцент, кафедра менеджмента, бизнеса и администрации, Николаевский национальный аграрный университет, Николаев, Украина, email: h.fedosieieva@outlook.com, ORCID ID: https://orcid.org/0009-0009-3536-0173

Боднар Е. – кандидат наук, доцент, кафедра финансов, банковского дела и страхования, Николаевский национальный аграрный университет, Николаев, Украина, email: o-bodnar@hotmail.com, ORCID ID: https://orcid.org/0009-0006-3099-3076

Сухорукова А. – PhD, доцент, кафедра менеджмента, бизнеса и администрации, Николаевский национальный аграрный университет, Николаев, Украина, email: asukhorukova@outlook.com, ORCID ID: https://orcid.org/0009-0002-2550-1218

Агафонов А. – аспирант, Николаевский национальный аграрный университет, Николаев, Украина, email: aahafonov@hotmail.com, ORCID ID: https://orcid.org/0009-0005-8651-8197