FinTech

MDPI

Article

A Multi-Stage Framework for Examining the Internal Activity and Refinement of the Cybersecurity Risk Mitigation System in Financial-Banking Environments

Laurențiu-Constrantin Stama [1,2], Roxana-Mariana Nechita [1,2,*], Dana-Corina Deselnicu [2], Cătălin-George Alexe [2] and Cătălina-Monica Alexe [2]

[1] Doctoral School of Entrepreneurship, Engineering and Business Management, National University of Science and Technology POLITEHNICA Bucharest, 060042 Bucharest, Romania; constantin.stama@upb.ro
[2] Department of Entrepreneurship and Management, Faculty of Entrepreneurship Business Engineering and Management, National University of Science and Technology POLITEHNICA Bucharest, 060042 Bucharest, Romania; dana.deselnicu@upb.ro (D.-C.D.); catalin.alexe@upb.ro (C.-G.A.); catalina.alexe@upb.ro (C.-M.A.)
* Correspondence: roxana.nechita@upb.ro

Abstract

The rapid digitalization of financial banking services has increased the need for effective cybersecurity risk mitigation as institutions rely on interconnected digital infrastructures. Understanding how technological, organizational, and human-related factors interact is important for supporting cybersecurity planning and risk management. This study examines the internal structure of cybersecurity risk mitigation in financial banking systems through a framework that combines bibliometric analysis, the Decision Making Trial and Evaluation Laboratory (DEMATEL) method, and the Matrix Impact Cross-reference Multiplication Applied to Classification (MICMAC) technique. The bibliometric analysis identified the factors most frequently associated with cybersecurity risk mitigation in scientific publications indexed in the Web of Science Core Collection. These factors were subsequently evaluated by a panel of IT and cybersecurity experts from the banking sector. DEMATEL was applied to examine the influence relationships among the identified factors, and MICMAC was used to refine the system by classifying the factors according to their driving and dependence power. The analysis provides a structured representation of the cybersecurity risk mitigation system and clarifies the role of each factor within the overall structure. The proposed framework may support managers, cybersecurity specialists and decision makers in cybersecurity planning, resource allocation, and strategic decision making within financial institutions.

Keywords: financial banking systems; DEMATEL; MICMAC; bibliometric analysis; cyber risk management; digital transformation; decision-making

JEL Classification: G32

Academic Editor: Shyan-Ming Yuan

Received: 31 July 2026
Revised: 14 September 2026
Accepted: 15 September 2026
Published: 15 September 2026

1. Introduction

The financial and banking sector has undergone major digital transformation during the last decades. Banking operations that were previously limited to physical infrastructures and direct institutional interaction are now strongly connected to digital technolo-

gies, online platforms, cloud environments, mobile applications, automated financial services, and interconnected payment systems [1]. Financial institutions increasingly depend on digital infrastructures for transaction processing, customer communication, data storage, authentication procedures, risk monitoring, and service delivery. The expansion of digital financial ecosystems has created new opportunities for operational efficiency and accessibility, yet it has also increased the exposure of banking systems to cybersecurity risks [2–4].

Cybersecurity incidents affecting financial institutions have become a persistent concern across both developed and developing economies. Cyberattacks directed toward financial systems frequently target customer data, financial transactions, authentication systems, payment infrastructures, communication networks, and institutional databases. Financial institutions remain attractive targets because of the high economic value of digital assets, the concentration of sensitive information, and the possibility of disrupting critical financial operations [3,5]. The increasing sophistication of cyber threats has further complicated the capacity of institutions to maintain secure digital environments.

The problem manifests itself in different forms across financial-banking systems. Unauthorized access incidents may compromise customer information and institutional records [6,7]. Malware and ransomware attacks may interrupt banking operations and generate substantial financial losses. Phishing campaigns continue to affect both customers and employees through fraudulent communication practices designed to obtain confidential information. Weaknesses in digital infrastructures, insufficient protection mechanisms, limited employee awareness, outdated technologies, and poor integration between security procedures may increase institutional vulnerability to cyber threats [3]. The integration of fintech services and third-party technologies into banking infrastructures has also created additional security challenges because vulnerabilities can spread through interconnected systems and external digital services [8,9].

Cybersecurity risks in financial systems intensified during periods characterized by rapid digital adoption and increased online financial activity. The expansion of remote banking services, mobile payment systems, digital wallets, and cloud-based financial operations has widened the attack surface available to cybercriminals. The accelerated use of digital financial technologies during periods of social and economic disruption further increased institutional dependence on online infrastructures and electronic services [1]. Under these conditions, financial institutions have been required to continuously adapt cybersecurity strategies, protection mechanisms, and risk management procedures in order to preserve operational continuity and customer trust [7].

The consequences of cybersecurity incidents extend beyond direct financial losses. Security breaches may affect institutional reputation, customer confidence, regulatory compliance, operational stability, and the reliability of digital financial services. Disruptions affecting payment infrastructures or banking networks may produce broader economic effects because financial systems support commercial transactions, investment activities, credit operations, and public financial interactions [10]. Cybersecurity problems within financial systems therefore affect financial institutions, customers, technology providers, regulatory authorities, businesses, and the wider economic environment [7,10].

The growing importance of cybersecurity in financial systems has generated increasing research interest in recent years. Existing studies examine topics such as information security, cyber risk management, digital banking protection, data privacy, technological vulnerabilities, financial technology security, blockchain security, artificial intelligence (AI) applications in cybersecurity, and institutional resilience strategies [11,12]. Research has also explored regulatory frameworks, cyber governance structures, employee awareness programs, intrusion detection systems, and encryption technologies used to improve digital security in financial environments.

Despite the increasing volume of studies related to cybersecurity and financial technologies, several limitations remain visible in the existing literature. Many studies approach cybersecurity risks from isolated technical perspectives and focus on specific technologies, attack methods, or protection mechanisms. Other studies examine organizational or regulatory aspects without analyzing the interaction between the multiple factors that shape cybersecurity risk mitigation within financial-banking systems [7,12]. The literature contains limited research dedicated to understanding how technological, organizational, operational, strategic, and human-related factors interact within a broader cybersecurity mitigation structure.

Another limitation concerns the fragmentation of the research field. Cybersecurity, cyber risk management, financial technologies, resilience strategies, and digital banking security are often discussed as separate thematic areas [13]. This fragmentation complicates the identification of the factors that exert the strongest influence on cybersecurity risk mitigation processes within financial systems. It also limits the possibility of distinguishing between driving factors, dependent factors, and secondary elements within the cybersecurity mitigation structure.

A clearer understanding of the relationships between cybersecurity mitigation factors is important for both academic research and institutional decision-making. Financial institutions operate within interconnected technological environments where changes affecting one component may influence other components of the system. The identification of highly influential factors may support the prioritization of cybersecurity investments, the adaptation of institutional strategies, the improvement of risk management procedures, and the development of more effective resilience mechanisms. At the same time, identifying factors with limited influence may support the refinement of cybersecurity systems and reduce unnecessary complexity in institutional security structures [13].

The present study addresses these issues through a combined bibliometric and multicriteria decision-making (MCDM) framework focused on cybersecurity risk mitigation in financial-banking systems. The study aims to identify the main factors associated with cybersecurity risk mitigation, to examine the relationships between these factors, and to refine the factor structure according to the influence and dependence levels observed within the system.

The first stage of the research is based on bibliometric analysis conducted using scientific publications indexed in the Web of Science Core Collection database. The bibliometric stage focuses on identifying the dominant research directions associated with cybersecurity risk mitigation in financial systems and on extracting the factors most frequently connected to this research area. The search strategy integrates concepts related to cybersecurity, cyber risks, mitigation processes, and financial-banking infrastructures in order to capture the interdisciplinary structure of the field. The bibliometric analysis includes overlay visualization and density visualization based on all keywords extracted from the selected scientific literature. Overlay visualization is employed to observe the evolution of research interests and thematic developments within the field. Density visualization is used to identify areas characterized by high keyword concentration and stronger thematic connectivity. The use of all keywords supports a more detailed identification of the factors associated with cybersecurity risk mitigation because keyword structures frequently reflect the conceptual priorities present within scientific research.

The factors extracted during the bibliometric stage are further examined through the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method. DEMATEL supports the analysis of causal relationships between factors and facilitates the identification of direct and indirect influences within the system [14]. This method makes it possible to distinguish between influential factors and dependent factors according to the intensity

of their interactions. This stage contributes to the understanding of how cybersecurity mitigation factors interact within financial-banking systems.

The Matrix Impact Cross-reference Multiplication Applied to Classification (MICMAC) method is subsequently applied in order to classify the identified factors according to their driving and dependence power. MICMAC analysis supports the refinement of the system by differentiating between autonomous, dependent, linkage, and driving factors [15]. This process contributes to the identification of factors that exert limited influence within the system structure and facilitates the clarification of the internal dynamics associated with cybersecurity risk mitigation.

The integration of bibliometric analysis with DEMATEL and MICMAC methods allows the study to move beyond simple literature description and toward the examination of relationships existing between cybersecurity mitigation factors [13]. The combination of these approaches supports both the identification of relevant factors and the analysis of their interaction within the broader financial-banking cybersecurity environment [14–16].

The expected results of the study include the identification of the principal factors associated with cybersecurity risk mitigation in financial-banking systems, the clarification of the causal relationships existing between these factors, and the classification of factors according to their role within the system structure. The findings are expected to contribute to a better understanding of cybersecurity mitigation processes in digital financial environments and to support future research related to cyber risk management, financial system resilience, and digital security strategies.

The study also provides practical relevance for financial institutions and decision-makers interested in strengthening cybersecurity preparedness and improving institutional resilience against cyber threats. The identification of influential factors may support the development of more targeted cybersecurity strategies, while the refinement of the factor structure may facilitate more efficient resource allocation and strategic planning within financial-banking systems.

2. Materials and Methods

The present study applies a hybrid methodological framework designed to investigate the factors associated with cybersecurity risk mitigation in financial-banking systems and to examine the internal relationships that exist between these factors. The methodological structure combines bibliometric analysis with two multi-criteria decision-making methods, namely the DEMATEL method and the MICMAC technique.

The methodological sequence follows three successive stages. The first stage focuses on the identification and extraction of factors from the scientific literature through bibliometric analysis. The second stage examines the causal influence relationships between the extracted factors through DEMATEL analysis. The third stage applies MICMAC in order to refine the factor structure according to the driving and dependence power of each factor within the cybersecurity mitigation system.

The selection of this methodological combination is linked to the complexity of cybersecurity environments in financial systems [15]. Cybersecurity mitigation in banking infrastructures depends on multiple interconnected technological, organizational, operational, and strategic elements. Changes affecting one component of the system may generate influence chains across several related areas. Under these conditions, conventional ranking methods provide limited insights into underlying structural interactions [14,17]. The integration of bibliometric analysis with DEMATEL and MICMAC methods supports the transition from factor identification toward the examination of systemic interaction patterns and structural influence mechanisms.

2.1. Bibliometric Analysis

Bibliometric analysis was selected as the first stage of the research because it allows the examination of a large scientific literature base and facilitates the extraction of the factors most frequently associated with cybersecurity mitigation in financial-banking systems. The method reduces subjective factor selection and supports the identification of concepts that appear consistently across the scientific literature.

The scientific publications included in the analysis were retrieved exclusively from the Web of Science Core Collection database. This database was selected because it indexes peer-reviewed journals that pass strict editorial and scientific evaluation procedures. The database also offers stable citation indexing, standardized bibliographic information, and reliable keyword structures frequently used in management, information security, engineering, and financial system research.

The search strategy was structured around four thematic directions associated with cybersecurity mitigation in financial-banking environments. The first thematic direction focused on cybersecurity and information security concepts through terms associated with cyber security, digital security, computer security, information protection, and data security. The second thematic direction targeted cyber risk and technology-related risk concepts. The third thematic direction addressed mitigation and protection mechanisms through terms associated with prevention, management, resilience, protection, reduction, and control processes. The fourth thematic direction focused on financial-banking infrastructures through concepts associated with banking systems, financial technologies, payment systems, digital financial services, networks, and technological infrastructures.

The search formula was constructed with proximity operators in order to preserve semantic association between terms while avoiding restrictive fixed expressions:

$$\begin{gathered} TS = ((((cyber* \ OR\ information\ OR\ data\ OR\ computer\ OR\ digital*) \\ NEAR/4\ secur*)\ OR\ ((cyber* \ OR\ digital* \ OR\ technolog*)\ NEAR/4\ risk*)) \\ NEAR/6\ (mitigat* \ OR\ reduc* \ OR\ prevent* \ OR\ control* \ OR\ manag \\ * \ OR\ protect* \ OR\ resilien*) \\ NEAR/6\ (\ (bank* \ OR\ financ* \ OR\ credit* \ OR\ fintech* \ OR\ payment*) \\ NEAR/4\ (system* \ OR\ infrastructur* \ OR\ network* \ OR\ technolog \\ * \ OR\ service* \ OR\ platform*))) \end{gathered} \quad (1)$$

The use of proximity operators increased the flexibility of the retrieval process and allowed the identification of conceptually related terms appearing in different textual forms within titles, abstracts, and keywords.

The cybersecurity and information security-related search sequence generated 135,596 indexed publications. The cyber risk-related sequence produced 28,258 records. The mitigation and resilience-related sequence generated 24,350,265 publications, indicating the broad use of these concepts across multiple scientific fields. The financial-banking infrastructure and digital financial systems-related sequence produced 138,471 indexed records.

The relationships between the thematic groups were subsequently examined through pairwise intersections in order to evaluate the degree of integration between the research directions. The intersection between cybersecurity and cyber risk concepts generated 1244 publications. The combination between cybersecurity and mitigation-related concepts produced 23,421 records. The intersection between cybersecurity and financial-banking system concepts generated 475 publications. The association between cyber risk and mitigation-related concepts produced 7222 publications, while the relationship between cyber risk and financial-banking infrastructure concepts generated 661 publications. The intersection between mitigation-related concepts and financial-banking systems generated 155,999 publications.

The complete intersection integrating cybersecurity, cyber risk, mitigation processes, and financial-banking system concepts generated 283 indexed publications within the Web of Science Core Collection database. The comparatively reduced number of records obtained through the intersection of all conceptual directions indicates that the combined research area remains relatively narrow compared to the individual thematic domains. This result suggests the existence of a focused research niche situated at the intersection between cybersecurity mitigation and financial-banking infrastructures.

The selection, eligibility, screening, and inclusion stages of the scientific publications followed the PRISMA workflow presented in Figure 1. The identification stage started from the 283 records obtained through the complete search formula intersection. The first eligibility filter limited the publication period to the interval between 2016 and 2026. This temporal interval was selected because the financial sector experienced accelerated digital transformation during the last decade through the expansion of fintech services, cloud banking infrastructures, digital payment systems, mobile financial applications, and AI integration within financial operations. The same period also corresponds to the rapid growth of cybersecurity incidents targeting digital financial systems, including ransomware attacks, phishing campaigns, financial data breaches, and attacks directed toward payment infrastructures. Earlier publications frequently address cybersecurity from traditional information security perspectives that are less connected to the current digital financial ecosystem. Applying the publication year filter reduced the dataset from 283 to 216 eligible publications, resulting in the exclusion of 67 records.

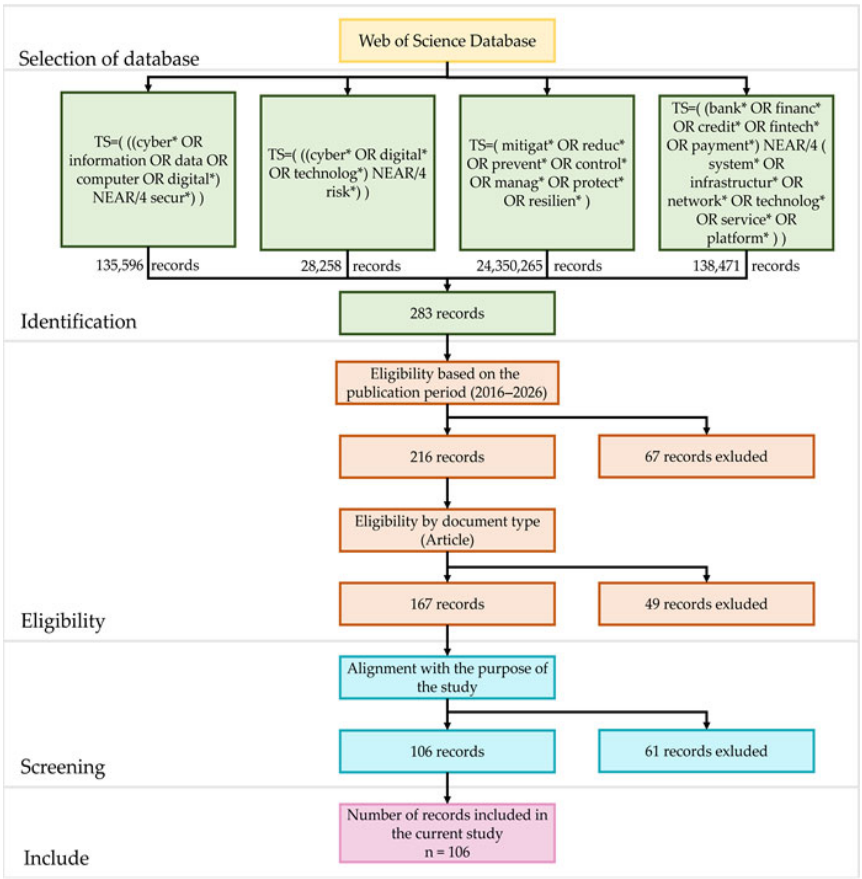

Figure 1. PRISMA Workflow.

The second eligibility stage restricted the dataset to publications classified exclusively as research articles. This filter was introduced in order to preserve original scientific

contributions and to reduce citation concentration bias associated with review papers. Review articles frequently summarize and repeatedly cite a limited group of original studies, which may artificially amplify the visibility of certain concepts or factors within bibliometric structures. Restricting the dataset to original articles supports a more balanced factor extraction process because the identified concepts originate directly from primary research contributions. After applying the document type filter, the dataset decreased from 216 to 167 eligible publications, leading to the exclusion of 49 records.

The screening stage focused on the alignment between the selected publications and the objective of the present study. Titles and abstracts were examined in order to identify studies directly associated with cybersecurity risk mitigation in financial-banking systems. Publications addressing unrelated technological fields, general information security topics without financial relevance, or studies lacking direct connection to cybersecurity mitigation were excluded during this stage. Publications carrying the "retracted" label within the Web of Science database were also removed from the dataset in order to preserve the scientific reliability of the analyzed literature. The screening process resulted in the exclusion of 61 publications.

The final dataset included 106 scientific articles used for the bibliometric analysis and subsequent factor extraction process.

Keyword co-occurrence analysis was conducted with VOSviewer software version 1.6.20. The analytical unit was defined as "All keywords" because this structure allows the identification of broader conceptual relationships present within the scientific literature. Overlay visualization analysis was employed in order to examine the temporal evolution of research interests associated with cybersecurity mitigation in financial systems. This stage facilitated the identification of themes that gained increasing scientific attention during recent years.

Density visualization analysis was subsequently applied in order to identify areas characterized by stronger conceptual concentration and higher thematic connectivity. The density structure supported the identification of the factors most frequently associated with cybersecurity mitigation in financial-banking systems and facilitated the extraction of the factors included in the following analytical stages.

The factors selected for DEMATEL and MICMAC analysis were extracted according to recurrence frequency, thematic relevance, and conceptual connectivity within the keyword network.

2.2. DEMATEL Method

After the bibliometric analysis and the extraction of the cybersecurity mitigation factors associated with financial-banking systems, the next stage of the research focused on examining the causal relationships within the model. This stage determines how factors interact, how influence propagates through the network, and which elements act primarily as cause or effect components. Managing cyber risks in financial infrastructures involves complex interactions among technological, operational, organizational, and strategic dimensions. Under these conditions, the behavior of the system cannot be understood through isolated factor evaluation because changes affecting one area may generate multiple indirect consequences throughout the entire structure.

The DEMATEL method was selected because it allows the analysis of causal influence relationships between interconnected factors. The method is particularly suitable for systems characterized by feedback effects, multidirectional influence propagation, and interaction chains extending beyond direct relationships. Financial-banking cybersecurity environments contain this type of structural complexity because cyber resilience, risk management procedures, technological infrastructure, operational monitoring, employee awareness, digital payment security, and governance mechanisms continuously affect one

another. A modification introduced in one area may therefore influence several related components inside the system.

The use of DEMATEL was also necessary because the objective of the present study is connected to the later refinement of the cybersecurity mitigation factor structure through MICMAC analysis. The purpose of the research is not limited to identifying important factors from the literature. The study also seeks to determine which factors maintain strong systemic activity, which factors shape the behavior of the remaining system components, and which factors exhibit limited structural contribution. DEMATEL provides the influence and dependence values necessary for this type of classification. The method therefore acts as the analytical foundation for the subsequent MICMAC stage, where the membership and non-membership of factors inside the cybersecurity mitigation system can be interpreted according to their structural behavior.

The DEMATEL evaluation process involved a panel of 15 experts specialized in information technology and cybersecurity risk management within the banking sector. The selected experts currently work in financial-banking institutions where their professional activity focuses on cyber risk assessment, digital infrastructure protection, information security management, and cybersecurity monitoring processes. A minimum professional experience of 5 years was established as an eligibility criterion. This threshold was selected to increase the likelihood that the experts had encountered, during their professional activity, cybersecurity risks with different levels of occurrence probability, including risks with a lower probability of materialization that may require a longer period of professional exposure to be observed in practice [18,19]. Their practical experience in managing cybersecurity challenges associated with banking systems provided the contextual knowledge necessary for evaluating the influence relationships between the extracted factors. The expert evaluations were collected during May and June 2026 and focused on identifying the intensity of influence exerted by one factor on another within the cybersecurity mitigation structure. Each expert evaluated the interaction relationships between factors through a five-point influence scale:

- 0 = no influence;
- 1 = weak influence;
- 2 = moderate influence;
- 3 = strong influence;
- 4 = very strong influence.

The use of this scale allowed the transformation of qualitative expert judgments into numerical influence values suitable for mathematical analysis. The individual evaluation matrices obtained from the experts were subsequently aggregated into a single direct relation matrix representing the initial interaction structure of the cybersecurity mitigation system.

The first mathematical stage of DEMATEL involves the construction of the direct relation matrix. This matrix reflects the direct influence relationships existing between all extracted factors. For each pair of factors, the individual influence scores assigned by the 15 experts were aggregated using the arithmetic mean, and the resulting mean value was used as the corresponding element of the direct relation matrix. Thus, each matrix element represents the mean intensity of the direct influence transmitted from one factor toward another factor. The resulting matrix provides the initial quantitative representation of the interaction structure characterizing cybersecurity risk mitigation in financial-banking systems.

The direct relation matrix is expressed as follows:

$$A = \begin{bmatrix} 0 & a_{12} & \cdots & a_{1n} \\ a_{21} & 0 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & 0 \end{bmatrix} \quad (2)$$

In this matrix, A represents the initial direct relation matrix describing the direct interaction structure between factors. The element a_{ij} represents the influence exerted by factor i on factor j, while n represents the total number of factors included in the analysis. The diagonal elements are equal to zero because a factor does not directly influence itself.

After constructing the direct relation matrix, the next mathematical stage involves matrix normalization. This stage is necessary because the original influence values may contain unequal scaling conditions generated by variations in expert scoring intensity. Certain factors may accumulate larger influence values simply because stronger numerical evaluations were assigned during the assessment process. Without normalization, these differences may distort the calculation of indirect relationships and influence propagation paths.

The normalization procedure transforms the matrix into a proportional structure where all values remain inside a controlled interval suitable for subsequent calculations. This operation ensures mathematical comparability between influence relationships and stabilizes the propagation process used during the calculation of indirect effects.

The normalized matrix is obtained through the following expression:

$$Y = A \cdot k \quad (3)$$

In this formula, Y represents the normalized direct relation matrix, A represents the initial direct relation matrix, and k represents the normalization coefficient used to proportionally scale the matrix values. The normalization coefficient is calculated through the following formula:

$$k = \frac{1}{max_{1 \le i \le n}\left(\sum_{j=1}^{n} a_{ij}\right)} \; (i, j = 1, 2, \ldots, n) \quad (4)$$

In this expression, k represents the normalization coefficient, a_{ij} represents the influence value between factor i and factor j, while $\sum_{j=1}^{n} a_{ij}$ represents the total influence exerted by factor i. The operator max identifies the largest row sum inside the matrix. The normalization procedure ensures that the highest cumulative influence value becomes equal to one, while the remaining values are proportionally reduced according to the same scaling ratio.

After normalization, the next objective of the DEMATEL procedure is the identification of indirect influence relationships. Direct influence alone cannot fully explain the behavior of cybersecurity mitigation systems because many interactions occur through intermediary factors. A factor may therefore influence another component indirectly through multiple interaction chains distributed across the system structure.

For example, cybersecurity governance mechanisms may indirectly affect operational resilience through employee awareness procedures, monitoring systems, and incident response structures. Similarly, digital infrastructure quality may indirectly influence cyber risk mitigation through threat detection capacity, operational continuity, and data protection mechanisms. The cybersecurity mitigation system therefore contains cumulative influence paths extending beyond immediate interactions.

In order to capture these propagation effects, DEMATEL calculates the total relation matrix T. This matrix integrates both direct and indirect influence relationships and provides a complete representation of influence circulation inside the system. The total relation matrix T is calculated through the following formula:

$$T = Y \cdot (I - Y)^{-1} \tag{5}$$

In this formula, T represents the total relation matrix containing all direct and indirect influence relationships, Y represents the normalized direct relation matrix, and I represents the identity matrix. The component $(I - Y)^{-1}$ represents the inverse matrix used for calculating cumulative influence propagation throughout the system.

The purpose of this mathematical operation is to capture the series of indirect interactions generated between factors. The resulting matrix therefore reflects both immediate causal relationships and all indirect influence chains transmitted through intermediary components. This stage is particularly important in cybersecurity mitigation analysis because financial-banking systems operate through interconnected digital environments where influence propagation frequently extends across multiple operational and technological layers.

After obtaining the total relation matrix, the next analytical stage involves identifying the most meaningful relationships inside the system. Complex systems usually contain numerous weak interactions characterized by limited influence intensity. Including all minor relationships inside the causal diagram may reduce readability and obscure the principal structural relationships defining the behavior of the cybersecurity mitigation system.

To address this issue, a threshold value (α) is calculated in order to retain the influence relationships exceeding the selected threshold and to exclude weaker interaction paths considered less relevant for the causal diagram.

The threshold value is calculated through the following expression:

$$\alpha = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} [t_{ij}]}{N} \tag{6}$$

In this formula, α represents the threshold value used for filtering the influence relationships, t_{ij} represents the influence value located inside the total relation matrix, and N represents the total number of matrix elements, including the diagonal elements. Since the matrix has n rows and n columns, $N = n^2$, where n is the total number of factors.

Relationships characterized by values below the threshold are excluded from the final causal diagram because they are treated as weaker interactions for the purpose of visualizing the main influence structure. The threshold stage is important because cybersecurity mitigation systems frequently generate many secondary influence paths that may complicate the interpretation of the system structure. Removing these weak relationships improves the visibility of the principal causal mechanisms shaping the behavior of the cybersecurity mitigation environment.

Once the relevant relationships are retained, the DEMATEL procedure continues with the calculation of the total influence exerted and received by each factor. This stage allows the identification of factors acting mainly as causal drivers and factors behaving mainly as receivers of influence.

The total influence exerted by each factor (D_i) is calculated through the row sums of the total relation matrix:

$$D_i = \left[\sum_{j=1}^{n} t_{ij} \right]_{nx1} = [t_i]_{nx1'} \tag{7}$$

D_i represents the total influence exerted by factor i, while t_{ij} represents the influence transmitted from factor i toward factor j. The value of D_i indicates the degree to which a factor affects the remaining components of the cybersecurity mitigation system.

The total influence received by each factor (R_j) is subsequently calculated through the column sums of the total relation matrix:

$$R_j = \left[\sum_{j=1}^{n} t_{ij}\right]_{1xn} = [t_j]_{nx1'} \quad (8)$$

R_j represents the total influence received by factor j, while t_{ij} represents the influence transmitted toward factor j. The value of R_j indicates the degree to which a factor depends on the remaining system components.

The next stage of the analysis focused on interpreting the systemic role of each factor based on the influence values obtained from the total relation matrix. Two indicators were subsequently derived from the calculated influence values in order to evaluate the position and behavior of each factor inside the cybersecurity mitigation system.

The first indicator, represented by the $D + R$ value, was obtained by combining the total influence exerted by a factor with the total influence received by the same factor. This value reflects the overall prominence of the factor inside the system and indicates the degree to which the factor participates in the interaction structure. Higher $D + R$ values suggest that the factor occupies a central position within the cybersecurity mitigation environment and maintains strong interaction relationships with the remaining system components.

The second indicator, represented by the $D - R$ value, was obtained by calculating the difference between the total influence exerted and the total influence received by each factor. This value was used to determine the causal orientation of the factor inside the system. Positive $D - R$ values indicate that the factor mainly acts as a causal driver capable of influencing other components of the cybersecurity mitigation structure. Negative $D - R$ values indicate that the factor mainly behaves as a receiver of influence generated by the remaining system elements.

The values obtained through these calculations supported the construction of the DEMATEL causal diagram and facilitated the interpretation of influence propagation throughout the cybersecurity mitigation structure associated with financial-banking systems.

The DEMATEL stage therefore provided the mathematical and conceptual basis necessary for the following MICMAC analysis. The method allowed the study to move beyond isolated factor evaluation toward the examination of systemic interaction patterns, influence circulation mechanisms, and structural activity inside the cybersecurity mitigation system.

2.3. MICMAC Technique

Built directly upon the DEMATEL total-relation matrix T, the MICMAC technique categorizes factors based on their systemic role. Without introducing new inputs, this step translates pairwise influence values into a functional classification based on driving power and dependence levels.

Driving power for each factor is obtained as the sum of each row of T, corresponding to D_i. This value shows how strongly a factor influences all other elements in the system. Dependence is obtained as the sum of each column of T, corresponding to R_j. This value shows how strongly a factor is influenced by the rest of the system.

Each factor is then placed on a two-axis diagram where the horizontal axis represents dependence (R_j) and the vertical axis represents driving power (D_i). This positioning allows a direct view of how each factor behaves inside the system and supports interpretation of its structural role.

The diagram is divided into four quadrants.

- Quadrant I (Linkage) includes factors with high driving power and high dependence (D_i high, R_j high). These factors are strongly connected in both directions and tend

to create feedback effects inside the system. Any change affecting them spreads through several parts of the structure.

- Quadrant II (Drivers) includes factors with high driving power and low dependence (D_i high, R_j low). These factors act as main sources of influence inside the system and shape the behaviour of other elements. They represent key drivers of the cybersecurity mitigation structure.
- Quadrant III (Autonomous) includes factors with low driving power and low dependence (D_i low, R_j low). These factors remain weakly connected to the system and show limited interaction with other components.
- Quadrant IV (Dependent) includes factors with low driving power and high dependence (D_i low, R_j high). These factors are mainly influenced by other elements and usually reflect outcomes generated within the system. The MICMAC diagram provides a structured way to interpret matrix T and supports the classification of factors according to their role in cybersecurity mitigation processes within financial banking systems.

The MICMAC diagram provides a structured way to interpret matrix T and supports the classification of factors according to their role in cybersecurity mitigation processes within financial banking systems.

Although MICMAC uses the same underlying relationship information as DEMATEL, its purpose in the present study is different. DEMATEL quantifies the causal influence structure through the D and R values, whereas MICMAC provides a visual classification of the factors according to their driving power and dependence. This visual representation makes it easier to distinguish factors that strongly influence the system, factors that are highly interconnected, and factors with relatively limited interaction with the remaining structure. Autonomous factors should therefore be interpreted as elements with comparatively low driving power and dependence, rather than as factors that are irrelevant or suitable for removal. Their classification may indicate that their influence is more limited or context-dependent within the analysed system. Thus, MICMAC is used as a complementary interpretative tool rather than as a separate source of causal information.

3. Results

This section presents the findings obtained through the multi-stage analytical framework applied to cybersecurity risk mitigation mechanisms within financial-banking environments. The procedure follows three consecutive stages: bibliometric mapping of the research field, structural modelling of factor interactions using the DEMATEL approach, and classification of system elements through the MICMAC method. The purpose of this section is to present the structure of the dataset, the variables used, and the resulting matrices before any form of interpretation is addressed in later sections.

3.1. Results of the Biblimetric Analysis

The first stage involved an initial exploration of the literature related to cybersecurity risk management in banking institutions. The objective of this step was to identify the main conceptual directions reflected in the existing research landscape. A keyword co-occurrence analysis was conducted using VOSviewer software, with the unit of analysis defined as all keywords extracted from the selected documents.

The dataset consisted of a filtered collection of scientific publications selected according to predefined inclusion criteria. From the total set of extracted keywords, only those meeting the minimum occurrence threshold were included in the mapping process. These

keywords were used to construct visual representations based on co-occurrence relationships, temporal evolution, and density distribution. The representation in Figure 2 shows the evolution of keywords over time based on publication year.

The color gradient reflects temporal distribution, where different shades indicate earlier or more recent research activity. This allows observation of how research attention shifts across different topics within the dataset.

A second visualization was generated in order to capture the density of keyword distribution across the dataset (Figure 3).

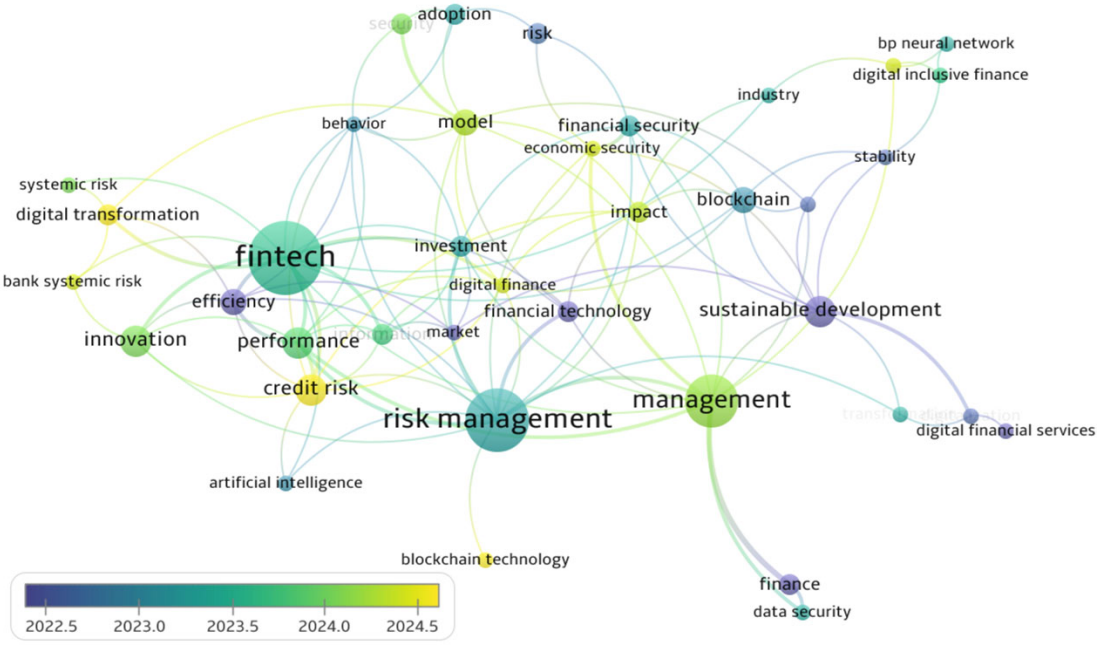

Figure 2. Keyword co-occurrence: overlay visualisation.

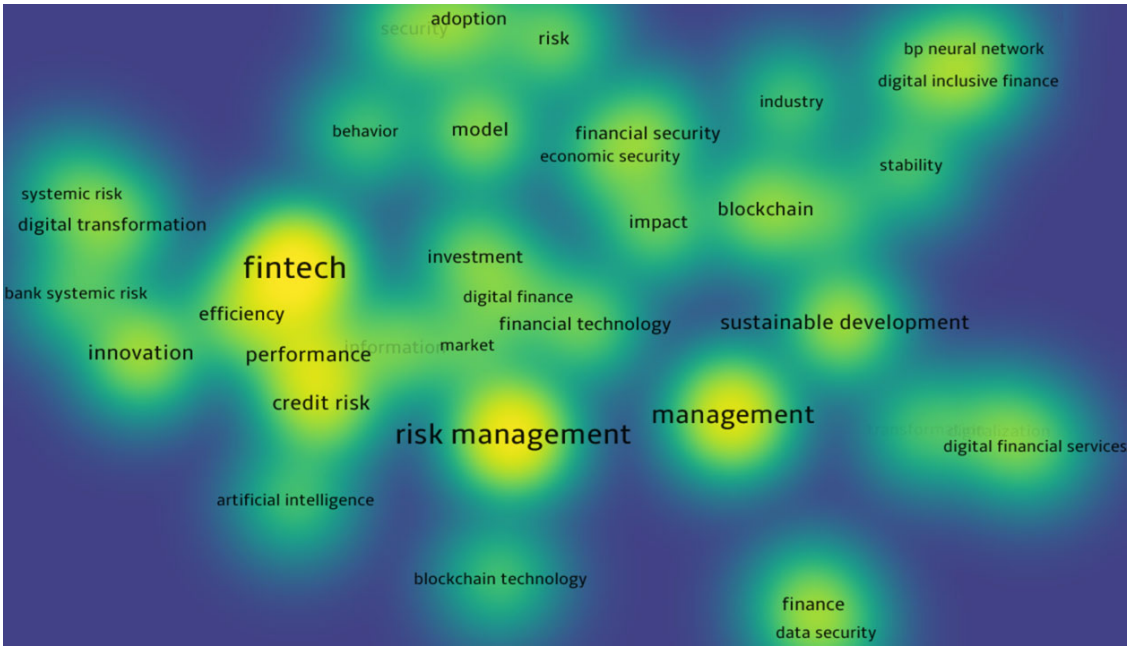

Figure 3. Keyword co-occurrence: density visualisation.

The density map in Figure 3 illustrates the concentration of keywords within the research field. Areas with higher intensity indicate regions where terms appear more frequently together, while lower intensity zones reflect more dispersed keyword usage across publications.

The bibliometric analysis was used as the starting point for identifying the concepts that received substantial attention in the analyzed literature. The occurrence and connectivity of keywords were considered as indicators of the visibility and thematic relevance of particular concepts within the research field, rather than as a ranking of their practical importance. The keywords identified in the bibliometric maps were therefore not directly transferred as individual factors. Some terms were too broad or context-dependent to represent a clearly defined component of a cybersecurity risk mitigation system. Related terms were consequently interpreted and grouped into broader conceptual dimensions according to their meaning, thematic relationships, and relevance to the objective of the study.

The grouping was based on three criteria. First, occurrence and thematic visibility were considered to identify concepts that were sufficiently represented within the analyzed literature and connected to the main themes of the keyword network. Second, conceptual relatedness among keywords was examined to determine whether different terms referred to the same or closely related underlying dimension. Third, relevance and interpretability for cybersecurity risk mitigation in financial-banking systems were considered to ensure that each resulting construct had a sufficiently clear meaning and could be consistently evaluated by the expert panel. Thus, keyword frequency alone was not used as a selection rule.

The resulting factors should therefore be understood as conceptual umbrellas derived from the bibliometric evidence rather than as individual bibliometric keywords. This distinction also means that the final factors do not have independent keyword occurrence frequencies. The frequencies observed in the bibliometric analysis refer to the individual keywords, whereas the eight factors were subsequently formulated by grouping related concepts into analytically defined constructs. This approach was adopted to avoid assigning a specific meaning to broad terms and to provide sufficiently clear factor definitions for the subsequent expert assessment.

The final set of factors is presented below:

- F_1—Digitalization level: the degree to which banking operations and services are implemented through digital platforms and electronic systems.
- F_2—Artificial intelligence integration: the extent of use of machine learning systems for detection, prediction, and response to cyber threats.
- F_3—Blockchain technology adoption: the level of implementation of distributed ledger systems for securing transactions and data integrity.
- F_4—Risk management system complexity: the structural depth of procedures, controls, and mechanisms used for identifying and managing cyber risks.
- F_5—System sustainability: the ability of the cybersecurity framework to maintain operational stability over time under changing external conditions.
- F_6—Regulatory compliance: the alignment of internal cybersecurity practices with applicable legal and supervisory requirements in the banking sector.
- F_7—Technical infrastructure resilience: the capacity of digital and physical infrastructure to maintain functionality during and after cyber incidents.
- F_8—Human factor awareness: the level of employee understanding and behavioral readiness regarding cybersecurity practices and threats.

These operational definitions were subsequently used to ensure a common interpretation of the eight constructs during the expert evaluation and DEMATEL analysis.

3.2. DEMATEL Results

In the second stage of the analysis, expert evaluations were collected in order to determine the direct influence relationships between the previously defined factors. Each expert completed a structured comparison between all pairs of variables based on the operational definitions provided during the preparation phase.

Before completing the evaluation matrices, the experts were introduced to the meaning of each factor in a controlled session designed to standardize understanding across participants. The results of this stage are organized in a sequence of matrices that represent direct and indirect relationships within the system.

The normalized direct relationship matrix is presented below (Table 1).

Table 1. Normalized direct relationship matrix.

Factor	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
F_1	0.000	0.112	0.119	0.143	0.155	0.119	0.152	0.109
F_2	0.112	0.000	0.085	0.137	0.131	0.106	0.122	0.097
F_3	0.082	0.073	0.000	0.109	0.112	0.106	0.125	0.061
F_4	0.112	0.116	0.094	0.000	0.152	0.158	0.146	0.134
F_5	0.155	0.097	0.103	0.128	0.000	0.122	0.179	0.109
F_6	0.103	0.091	0.091	0.161	0.143	0.000	0.106	0.134
F_7	0.146	0.094	0.103	0.143	0.179	0.137	0.000	0.088
F_8	0.100	0.097	0.052	0.146	0.128	0.128	0.112	0.000

The total-relation matrix (Table 2) is derived from the normalized matrix and includes both direct and indirect effects among variables. A α-threshold value is applied to distinguish relevant interactions from weaker connections within the system. Only values above this threshold are considered significant for system-level mapping.

Table 2. Total-relation matrix with relationships exceeding the selected threshold marked with (*) ($\alpha > 0.655$).

Factor	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
F_1	0.601	0.607	0.591	0.815 (*)	0.852 (*)	0.743 (*)	0.814 (*)	0.644
F_2	0.633	0.449	0.508	0.731 (*)	0.751 (*)	0.660 (*)	0.711 (*)	0.572
F_3	0.532	0.452	0.369	0.622	0.646	0.580	0.628	0.472
F_4	0.703 (*)	0.611	0.572	0.693 (*)	0.851 (*)	0.776 (*)	0.810 (*)	0.666 (*)
F_5	0.729 (*)	0.590	0.574	0.796 (*)	0.711 (*)	0.739 (*)	0.827 (*)	0.637
F_6	0.647	0.552	0.530	0.777 (*)	0.787 (*)	0.589	0.725 (*)	0.623
F_7	0.722 (*)	0.587	0.574	0.807 (*)	0.862 (*)	0.750 (*)	0.675 (*)	0.621
F_8	0.609	0.526	0.468	0.724 (*)	0.732 (*)	0.663 (*)	0.688 (*)	0.473

The sums of rows and columns from the total-relation matrix are used to compute two indicators for each factor: D, representing the total influence given, and R, representing the total influence received. These values are further used to determine prominence ($D + R$) and net influence ($D - R$), which support the construction of the causal structure.

The causal diagram (Figure 4) is generated based on the values contained in Table 3. The visualization presents directional links between factors, where only relationships exceeding the defined threshold are displayed.

Table 3. Assessment of the influence and causality of factors.

Factor	*D*	*R*	*D* + *R*	*D* − *R*	Net Characteristic
F_1	5.668	5.176	10.844	0.492	Cause
F_2	5.015	4.373	9.388	0.642	Cause
F_3	4.302	4.187	8.490	0.115	Cause
F_4	5.682	5.965	11.647	–0.284	Effect
F_5	5.604	6.192	11.796	–0.588	Effect
F_6	5.229	5.500	10.730	–0.271	Effect
F_7	5.597	5.878	11.475	–0.281	Effect
F_8	4.883	4.708	9.591	0.175	Cause

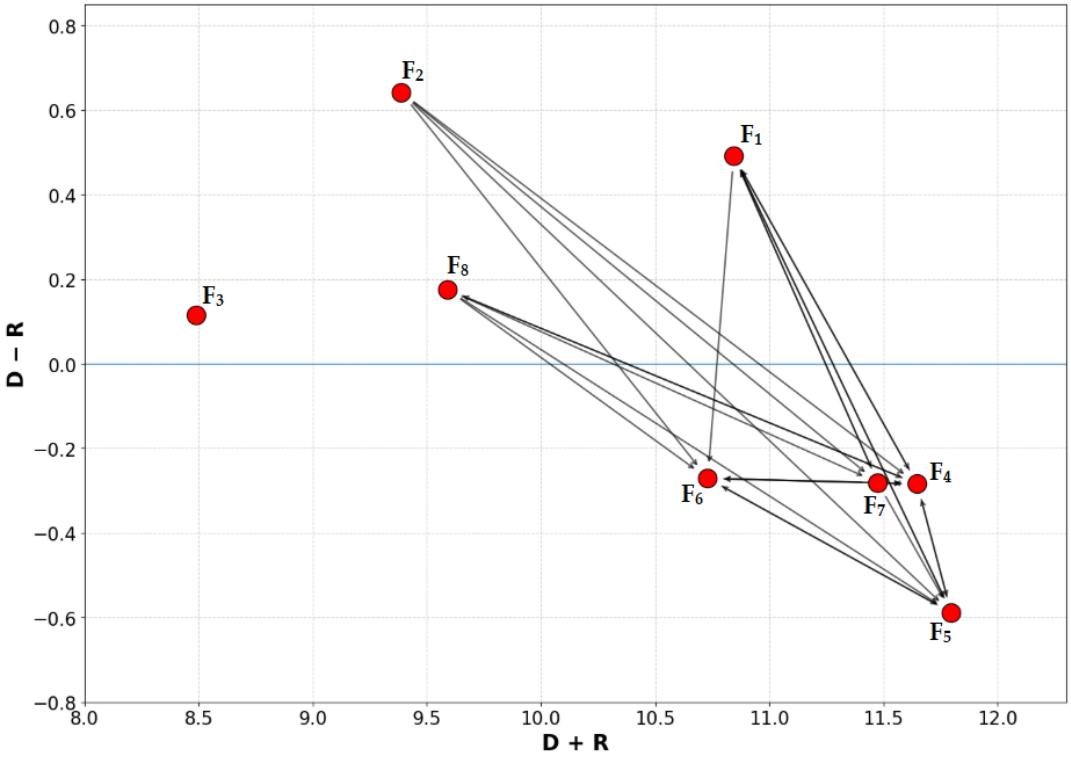

Figure 4. Causal diagram.

The diagram illustrates the structure of influence among variables, with directional arrows representing relationships derived from the total-relation matrix. The positioning of elements is based on computed prominence and net influence values.

3.3. MICMAC Results

The final stage of the analysis applies the MICMAC technique to classify the factors according to their driving power and dependence levels. Driving power is calculated from the sum of rows in the total-relation matrix, while dependence is obtained from the sum of columns.

These values are used to position each factor within a two-dimensional matrix (Figure 5) where the vertical axis represents driving power and the horizontal axis represents dependence. The resulting classification is displayed in a quadrant-based diagram.

The diagram divides the system into four categories using the mean values of *D* and *R* as the separation thresholds:

- Quadrant I (linkage factors): F_4, F_5, and F_7 are positioned in the linkage quadrant, showing both high driving power and high dependence. These factors are strongly

connected to the other elements of the system and may both influence and be influenced by changes occurring within the cybersecurity risk mitigation structure.

- Quadrant II (driving factors): F_1 is positioned in the strong drivers quadrant, with high driving power and relatively low dependence. This position indicates that digitalization level has a strong influence on the other factors while being less dependent on changes occurring elsewhere in the system. F_1 therefore represents an upstream factor within the cybersecurity risk mitigation structure.
- Quadrant III (autonomous factors): F_2, F_3, and F_8 are located in the autonomous quadrant, showing relatively low driving power and low dependence. These factors exhibit comparatively lower driving power and dependence than the factors positioned in the other quadrants. This classification reflects their relative position within the analysed system and does not imply that they are irrelevant to cybersecurity risk mitigation.
- Quadrant IV (dependent factors): F_6 is positioned in the dependent quadrant, with relatively low driving power and high dependence. This indicates that regulatory compliance is more strongly influenced by other elements of the cybersecurity risk mitigation system than it influences them directly.

The classification presented in Figure 5 provides a structured representation of how cybersecurity-related variables are distributed within the analytical framework. This layout serves as the final output of the quantitative modelling stage before further interpretation is conducted in subsequent sections.

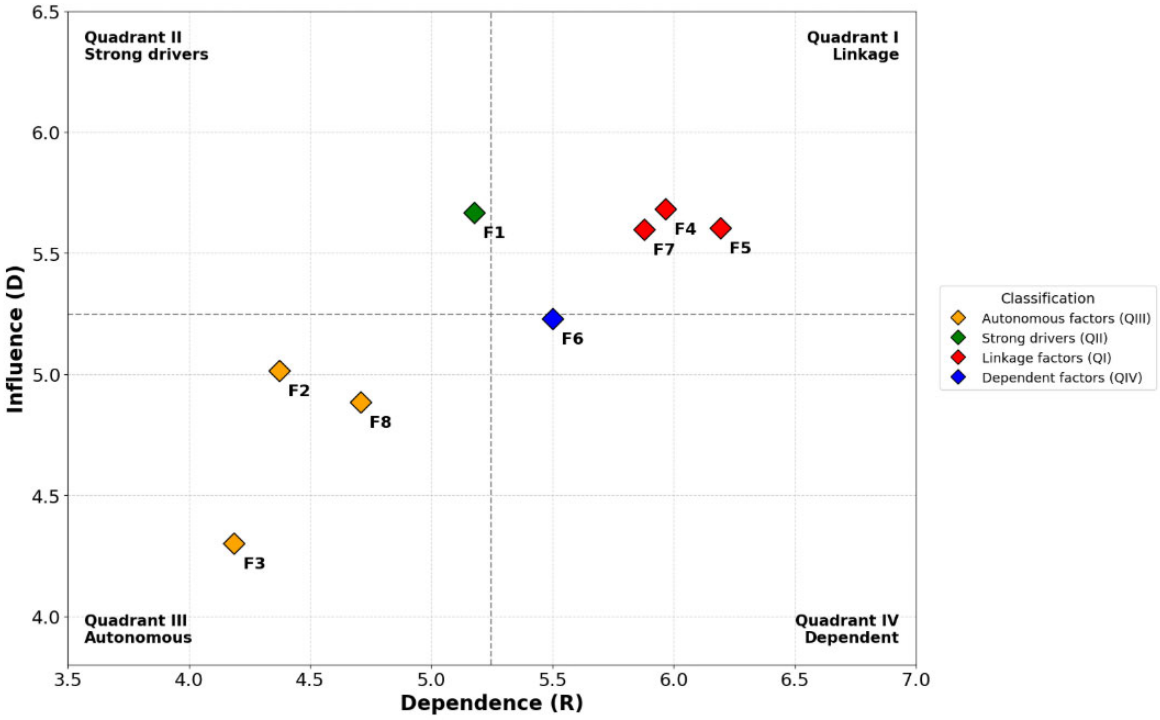

Figure 5. MICMAC diagram.

Although some factors have a cause characteristic according to DEMATEL, this does not necessarily mean that they have a high level of interaction with the entire system. DEMATEL identifies the net direction of influence through the $D - R$ value, while the overall level of interaction can be observed through the magnitude of the influence exerted and received, reflected by D, R, and their sum $D + R$. This distinction is particularly rel-

evant for F8. With $D = 4.883$ and $R = 4.708$, F_8 has relatively low levels of influence exerted and received compared with several other factors. Nevertheless, its $D - R$ value is positive (0.175), indicating that the influence exerted by F_8 is greater than the influence it receives. It can therefore be classified as a cause factor in DEMATEL while still having a comparatively limited level of overall interaction within the system. The MICMAC captures this second aspect by considering driving power and dependence and comparing their levels within the system. The autonomous position of F_8 should therefore be understood as an indication of its relatively limited system-wide interaction, rather than as an indication that the factor is unimportant.

The same distinction applies to F_2 and F_3. Their positive $D - R$ values of 0.642 and 0.115, respectively, indicate a net causal orientation, while their MICMAC autonomous classification reflects their comparatively lower levels of driving power and dependence. Thus, the two classifications address different aspects of the factor relationships. DEMATEL indicates whether a factor exerts more influence than it receives, whereas MICMAC indicates the strength of its driving and dependence position within the system. A positive net influence can therefore coexist with a relatively low overall level of interaction.

4. Sensitivity Analysis

To examine whether the DEMATEL results were influenced by the judgments of individual experts, a leave-one-expert-out (LOO) sensitivity analysis was performed. The analysis used the 15 individual questionnaires and recalculated the aggregated matrix and the DEMATEL results 15 times. In each iteration, one questionnaire was excluded and the remaining 14 questionnaires were used to obtain the arithmetic mean matrix. The DEMATEL procedure was then applied to each resulting matrix. This approach was selected to assess whether the classification and ranking of the factors remained stable when the assessment of one expert was removed from the dataset.

The dispersion of the individual judgments was also examined for the 56 off-diagonal relationships among the eight factors. The mean standard deviation was 0.98, the median standard deviation was 1.01, and the maximum standard deviation was 1.26. In addition, 72.86% of the individual ratings were within one point of the aggregated arithmetic mean, while 87.26% were within 1.5 points. These results indicate that differences existed between the experts' assessments, although most individual evaluations remained relatively close to the aggregated values. Table 4 summarizes the dispersion of the individual expert evaluations.

Table 4. Dispersion of the individual expert evaluations.

Measure	Value
Number of experts	15
Number of off-diagonal relationships	56
Mean standard deviation	0.98
Median standard deviation	1.01
Maximum standard deviation	1.26
Ratings within ±1 point of the aggregated mean	72.86%
Ratings within ±1.5 points of the aggregated mean	87.26%

The baseline DEMATEL results and the ranges obtained after excluding each expert in turn are presented in Table 5. The baseline $D - R$ values place F_1, F_2, F_3, and F_8 in the cause group, while F_4, F_5, F_6, and F_7 belong to the effect group. The sensitivity analysis produced the same classification in all 15 cases.

F_1 remained a cause factor in every sensitivity scenario, with $D - R$ values ranging from 0.424 to 0.614. F_2 also remained stable, with values between 0.523 and 0.728. F_3 showed the smallest positive net influence among the cause factors, with values ranging from 0.013 to 0.379. Although its lower bound was close to zero, F_3 remained in the cause group in all 15 analyses. F_8 also retained its cause classification, with $D - R$ values ranging from 0.042 to 0.205.

The effect factors remained stable as well. F_4 had $D - R$ values between −0.402 and −0.228, F_5 between −0.678 and −0.506, F_6 between −0.363 and −0.172, and F_7 between −0.386 and −0.192. Therefore, none of these factors changed from the effect group to the cause group in any of the sensitivity scenarios.

Table 5. LOO sensitivity analysis of the DEMATEL results.

Factor	Baseline $D - R$	LOO Min. $D - R$	LOO Max. $D - R$	Baseline Group	Cause Classification	Effect Classification
F_1	0.492	0.424	0.614	Cause	15/15	0/15
F_2	0.642	0.523	0.728	Cause	15/15	0/15
F_3	0.115	0.013	0.379	Cause	15/15	0/15
F_4	−0.284	−0.402	−0.228	Effect	0/15	15/15
F_5	−0.588	−0.678	−0.506	Effect	0/15	15/15
F_6	−0.271	−0.363	−0.172	Effect	0/15	15/15
F_7	−0.281	−0.386	−0.192	Effect	0/15	15/15
F_8	0.175	0.042	0.205	Cause	15/15	0/15

The sensitivity analysis confirms that the causal structure obtained from the aggregated matrix is stable across the 15 expert-exclusion scenarios. F_1, F_2, F_3, and F_8 consistently remain in the cause group, whereas F_4, F_5, F_6, and F_7 consistently remain in the effect group. The variations observed in the $D - R$ values reflect differences in individual expert judgments, but they do not alter the main causal interpretation of the model. The aggregated matrix can therefore be retained as the basis for the subsequent MICMAC analysis and the interpretation of the factor relationships, since the LOO results did not change the DEMATEL cause–effect classification.

5. Discussion

Combining bibliometric mapping with DEMATEL and MICMAC provides a structured view of the mechanisms shaping cyber risk mitigation in banking. While the eight core constructs align with broader literature trends, their relative causal positioning clarifies key operational interdependencies. This section examines these findings against studies published mainly between 2021 and 2026, focusing on how the current analysis positions the factors within ongoing debates about technology adoption, organizational practices, and risk management in banking.

The bibliometric stage highlighted persistent themes around digital transformation and security in banking. Overlay and density visualizations showed clusters centered on technology integration and human elements, consistent with patterns reported in reviews of the field. For instance, research on digitalization in banking frequently notes its dual role as both an enabler of efficiency and a source of new vulnerabilities. In the present study, digitalization level (F_1) emerged as a cause factor with notable prominence in the DEMATEL results. This finding matches observations that broader digital adoption expands the attack surface while simultaneously driving the need for stronger protective measures. Studies from the early 2020s [20,21] document how the shift to online and mobile banking during periods of disruption amplified exposure to threats, supporting the positioning of F_1 as an influential driver rather than a mere outcome.

Artificial intelligence integration (F_2) also appeared among the cause factors. Expert evaluations placed it as exerting influence on several other elements, including risk management and infrastructure resilience. This aligns with work that examines AI's role in threat detection and predictive analytics within financial institutions. One analysis using cognitive mapping and DEMATEL in the banking context similarly identified AI-related elements as central to addressing cybersecurity alongside digital transformation. Recent papers emphasize that AI tools help institutions move from reactive to proactive security postures, yet they also introduce complexities around data quality and model explainability [20]. The causal orientation of F_2 here reinforces the idea that AI acts more as an upstream influence than a dependent outcome, though implementation challenges remain.

Blockchain technology adoption (F_3) belongs to the cause group according to the DEMATEL results, although its net influence remains relatively low. An important finding is that F_3 does not exhibit any influence relationship exceeding the threshold value in the causal diagram. This indicates that blockchain technology adoption remains relatively isolated within the cybersecurity risk mitigation system and does not participate in the main influence pathways connecting the other factors. In practical terms, changes in blockchain adoption are not associated with influence relationships exceeding the selected threshold in the analysed system. This result suggests that, within the expert-assessed structure, blockchain technology adoption functions as a comparatively isolated component whose influence is less visible in the main pathways of the system. Recent studies acknowledge its potential to improve transaction integrity, transparency, and security in financial services, although implementation continues to be influenced by integration costs, regulatory uncertainty, and differences in organizational readiness [22,23]. The present findings indicate that blockchain has recognized value in financial banking cybersecurity, although it does not currently represent a significant structural driver of the cybersecurity risk mitigation system.

Risk management system complexity (F_4) fell into the effect category in the DEMATEL analysis. This suggests it responds to changes in upstream factors such as digitalization and regulatory demands. Such positioning finds support in studies that treat complex risk frameworks as outcomes shaped by technological and external pressures. For example, research on banking risk practices [24–26] highlights how evolving threat landscapes and compliance requirements drive increases in procedural depth, sometimes leading to operational burdens [27,28]. The findings here indicate that while sophisticated risk systems are necessary, their effectiveness depends heavily on the quality of driving factors like infrastructure and awareness.

System sustainability (F_5) and technical infrastructure resilience (F_7) both registered as effect factors with high prominence. Their dependence on other elements echoes discussions in resilience literature, where the ability to maintain operations under stress is viewed as the result of foundational investments in technology and governance [29]. Reports on financial system stability frequently link sustained performance to the interplay of digital tools and adaptive capacities, rather than treating resilience as an independent driver [30,31]. The MICMAC further clarifies these roles by placing certain factors in dependent or linkage quadrants, underscoring their sensitivity to broader system dynamics.

Regulatory compliance (F_6) appeared as an effect factor. This outcome aligns with analyses showing that compliance often follows from technological capabilities and risk management maturity rather than leading them outright. Recent examinations of banking regulations [31] note that while frameworks like those from supervisory authorities set minimum standards, actual adherence levels reflect internal readiness in areas such as

infrastructure and staff preparedness. The present study's results suggest that strengthening upstream drivers may improve compliance outcomes more effectively than isolated regulatory efforts.

Human factor awareness (F_8) stood out as a cause factor. Expert assessments indicated it influences multiple downstream elements, including risk management and sustainability. This finding is consistent with a growing body of evidence that positions employee behavior as a critical leverage point in cybersecurity. Human errors or lapses contribute to a substantial share of incidents in financial settings, often outweighing purely technical failures. Training programs and awareness initiatives appear repeatedly as recommended interventions, supporting the causal role identified here [32]. The results reinforce that awareness efforts can propagate improvements across the system when integrated with technological measures.

Overall, the DEMATEL causal diagram illustrates clear distinctions between driving and receiving factors. Cause-group elements (F_1, F_2, F_3, F_8) tend to shape the environment in which mitigation occurs, while effect-group factors (F_4–F_7) reflect the state of the system at a given time. This pattern matches broader calls in the literature for holistic approaches that address root influences rather than symptoms alone.

The MICMAC diagram complements these insights by mapping the factors according to their driving power and dependence. The linkage factors (F_4, F_5, and F_7) indicate elements with strong connections in both directions, while F_1 is positioned as a strong driving factor. F_2, F_3, and F_8 fall into the autonomous quadrant, whereas F_6 appears as a dependent factor. This classification provides an additional perspective on the structural position of each factor within the cybersecurity risk mitigation system.

Earlier assessments of electronic security risks in financial transactions, such as the framework developed by Glaessner, Kellermann and McNevin [33], focused on foundational pillars required to build a secure electronic environment. These included the legal framework and enforcement, the electronic security of payment systems, supervisory and prevention challenges, the role of private insurance, certification and standards, improved information sharing on security incidents, and education as a key preventive measure. In that period, the emphasis was placed on basic risk-management principles proportional to transaction value and on emerging threats such as identity theft, insider abuse, fraud and denial-of-service attacks. In contrast, the present multi-stage analysis identifies a more differentiated causal structure. Digitalisation level (F_1) emerges as a strong driving factor, while artificial intelligence integration (F_2) and human factor awareness (F_8) also act as causal elements. Risk-management system complexity (F_4), system sustainability (F_5) and technical infrastructure resilience (F_7) appear as linkage factors, and regulatory compliance (F_6) is positioned as a dependent outcome. This comparison illustrates the shift from relatively discrete foundational concerns toward a tightly interconnected configuration shaped by accelerated digital transformation.

A complementary perspective is offered by more recent work that classifies organisational responses according to financial constraints. Burtescu [34] distinguishes three practical approaches (minimum, optimal and imposed security) determined by the organisation's understanding of risk and its available funding. Minimum security corresponds to low maturity levels and is frequently observed when resources are insufficient, while optimal security follows a cost–benefit logic and imposed security arises when allocated funds fall short of calculated needs. In contrast to these resource-driven classifications, the present framework reveals that cybersecurity risk mitigation in financial-banking systems is structured around a small set of upstream drivers. Digitalisation level (F_1) exerts strong influence with relatively low dependence; artificial intelligence integration (F_2) and human factor awareness (F_8) act as additional causal factors; and the linkage group (F_4, F_5, F_7) shows high bidirectional connectivity. These findings suggest that effective mitigation

depends less on isolated budgetary decisions and more on the prioritisation of structural drivers that propagate influence throughout the system.

A further relevant perspective comes from research on the psychological dimension of financial decision-making. Gâdoiu [35] highlights that managers frequently rely on personal beliefs, perceptions, emotions and subjective interpretations when processing complex information, rather than on purely rational analysis. Cognitive biases, overconfidence, loss aversion and emotional states can therefore distort risk assessments and resource-allocation choices. In the present study, human factor awareness (F_8) emerges as a causal driver within the cybersecurity risk mitigation system. This positioning is consistent with the behavioural evidence that employee and managerial awareness, shaped by psychological factors, can exert upstream influence on risk-management practices, system sustainability and overall cyber resilience. The finding reinforces the need to treat the human component not merely as a residual vulnerability but as an active structural element capable of propagating improvements across the cybersecurity framework.

The present study contributes to the literature in several ways. First, it combines bibliometric mapping with structural modeling to derive factors empirically from recent publications rather than relying solely on expert opinion or narrow case studies. Second, the application of DEMATEL and MICMAC to this specific intersection of cybersecurity and financial-banking contexts offers a refined view of influence flows that goes beyond simple rankings. Third, the emphasis on cause–effect dynamics provides actionable insights for institutions seeking to allocate resources more effectively, with particular attention to system-level drivers such as digitalization and to human awareness as a causal factor that should remain part of cybersecurity planning.

These contributions address gaps noted in fragmented research that examines technologies or regulations in silos. By clarifying interdependencies, the analysis helps bridge technical, organizational, and human dimensions in a way that supports both academic understanding and practical decision-making.

Future research could extend this work in several directions. Longitudinal studies might track how factor relationships evolve as new technologies, such as advanced AI or quantum-resistant cryptography, enter banking environments. Comparative analyses across different regulatory jurisdictions or institution sizes would test the generalizability of the current classification. Incorporating quantitative performance metrics alongside expert judgments could further validate the model. Additionally, exploring interactions with emerging threats like AI-powered attacks or supply-chain vulnerabilities would keep the framework relevant. Researchers might also apply similar hybrid methodologies to other critical sectors to identify common patterns or sector-specific nuances.

In summary, the results show that cybersecurity risk mitigation is shaped by a set of factors with different causal and structural roles. Some factors exert stronger system-level influence, while others have a causal orientation within a more limited pattern of interactions. This perspective adds depth to existing literature and offers a basis for more targeted strategies in financial institutions.

6. Conclusions

This study examined the internal structure of cybersecurity risk mitigation in financial-banking environments through a framework that combines bibliometric analysis, DEMATEL, and MICMAC. It identified the main factors discussed in the scientific literature, examined the influence relationships among them, and classified their role within the overall system.

The findings show that cybersecurity risk mitigation depends on the interaction of technological, organizational, and human-related factors. Digitalization level, AI integra-

tion, blockchain technology adoption, and human factor awareness belong to the DEMATEL cause group, indicating that the influence exerted by these factors exceeds the influence they receive. Their MICMAC positions, however, show that F_2, F_3, and F_8 have comparatively lower levels of driving power and dependence within the system. Risk management system complexity, system sustainability, regulatory compliance, and technical infrastructure resilience belong to the DEMATEL effect group and are more strongly shaped by changes in the rest of the system.

The main contribution of this study lies in the integration of three complementary methods into a single analytical framework dedicated to cybersecurity risk mitigation in financial-banking environments. The bibliometric stage provided a structured process for identifying the relevant factors from the scientific literature, while the DEMATEL and MICMAC analyses explained how these factors interact and how they are positioned within the system. This approach offers a clear view of the relationships between the identified factors and supports a better understanding of their influence on cybersecurity risk mitigation.

The originality of the study comes from the way these methods are combined to examine cybersecurity risk mitigation in the financial-banking sector. Previous studies often focused on individual technologies, specific security measures, or separate organizational aspects. This study brings these elements together within a single framework that explains both the relationships among the factors and their structural position inside the system. The use of bibliometric analysis as the starting point for factor identification also provides a transparent basis for the subsequent stages of the analysis.

The results may be useful for several categories of stakeholders. Researchers can use the proposed framework as a reference for future studies on cybersecurity risk mitigation and for similar analyses in other critical sectors. Managers and decision makers in financial institutions can use the findings to support strategic planning and to identify the factors that deserve greater attention when strengthening cybersecurity capabilities. The framework may also be relevant for cybersecurity specialists, risk management professionals, and regulatory authorities interested in understanding how different components of the cybersecurity system influence one another.

The practical value of the study comes from its ability to support decision making. The combined interpretation of influence direction and driving-dependence position helps organizations distinguish between factors that exert a net causal influence and factors that have stronger system-level driving or dependence roles. The classification of factors according to their influence and dependence helps organizations distinguish between upstream drivers, highly interconnected factors, dependent outcomes, and factors with comparatively limited system-wide interaction. This information can support the planning of security investments, the development of employee awareness programs, the improvement of governance practices, and the design of cybersecurity strategies that are consistent with the characteristics of financial-banking environments.

Like any study, this research has several limitations. The bibliometric analysis was based only on publications indexed in the Web of Science Core Collection, meaning that relevant studies available in other scientific databases were not considered. This may introduce a degree of database-related bias, while the visibility of certain keywords may also be influenced by periods of increased academic interest in specific topics. Therefore, the prominence of a concept in the bibliometric analysis should not be interpreted directly as an indication of its practical importance for cybersecurity risk mitigation.

The DEMATEL analysis relied on the judgments of a panel of experts from the financial-banking sector, and the results reflect their professional experience and assessment of the relationships among the identified factors. The findings are therefore linked to the context examined in this study and should be interpreted with this aspect in mind. In

addition, the proposed framework represents the relationships between the selected factors within the study period. Changes in cybersecurity technologies, regulatory requirements, and the threat landscape may modify these relationships over time. In particular, the increasing use of new security approaches, including autonomous security-oriented agents, may influence the visibility and structural role of particular factors. The present study does not provide a separate comparison between different time periods; therefore, future research could examine the stability of the identified relationships through longitudinal analyses.

Future research can extend this work by applying the proposed framework to different countries or financial systems in order to examine possible differences between institutional and regulatory environments. Additional studies may include a larger panel of experts, incorporate new cybersecurity technologies as they become widely adopted, or compare financial institutions of different sizes. The framework may also be applied to other sectors that rely on complex digital infrastructures, such as healthcare, energy, telecommunications, or public administration, to examine whether similar influence patterns are observed.

Author Contributions: Conceptualization, L.-C.S. and R.-M.N.; methodology, L.-C.S., R.-M.N., D.-C.D., C.-G.A. and C.-M.A.; software, L.-C.S. and R.-M.N.; validation, D.-C.D. and C.-M.A.; formal analysis, R.-M.N.; investigation, L.-C.S.; resources, D.-C.D., C.-G.A. and C.-M.A.; data curation, D.-C.D., C.-G.A. and C.-M.A.; writing—original draft preparation, L.-C.S. and R.-M.N.; writing—review and editing, L.-C.S., R.-M.N., D.-C.D., C.-G.A. and C.-M.A.; visualization, R.-M.N.; supervision, D.-C.D., C.-G.A. and C.-M.A.; project administration, D.-C.D.; funding acquisition, D.-C.D., C.-G.A. and C.-M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National University of Science and Technology POLITEHNICA Bucharest through the PubArt programme.

Institutional Review Board Statement: Ethical review and approval were waived for this study by Institution Committee due to Legal Regulations (https://upb.ro/wp-content/uploads/2025/03/Regulament-Subcomisie-de-Bioetica_FINAL.pdf), accessed on 19 May 2026 (Art. 3 Studiile/Cercetările care implică subiecți umani sau animale).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: This work has been supported by: ERASMUS-EDU-2023-EUR-UNIV, Project 101124676—EELISA, funded by the European Union, https://eelisa.eu/ (accessed on 14 September 2026). Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. The authors also acknowledge the use of DeepL version: Translate and DeepL version: Write—AI-powered edits for the translation of the manuscript from Romanian to English, last accessed on 18 May 2026. Furthermore, the authors acknowledge the use of ChatGPT, version 5.3-mini to generate Python code (Python 3.11) for Figures 4 and 5. The authors significantly modified the generated code, specifically adjusting coordinates, colors, and font sizes, before executing it within a Google Colab environment. Data processing was performed using Microsoft Excel, part of the Microsoft Office Professional 2013 suite, version 15.0.5603.1000. The authors meticulously reviewed and edited the content to ensure accuracy and take full responsibility for the final manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ali, A.; Shah, M. What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector. *Information* **2024**, *15*, 760. https://doi.org/10.3390/info15120760.
2. Adekoya, O.A.; Atlam, H.F.; Lallie, H.S. Quantifying the Multidimensional Impact of Cyber Attacks in Digital Financial Services: A Systematic Literature Review. *Sensors* **2025**, *25*, 4345. https://doi.org/10.3390/s25144345.
3. Tran, T.N. Systematic Review of Cybersecurity in Banking: Evolution from Pre-Industry 4.0 to Post-Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice. *arXiv* **2025**, arXiv:2503.00070.
4. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors* **2023**, *23*, 6666. https://doi.org/10.3390/s23156666.
5. Kuzior, A.; Brożek, P.; Kuzmenko, O.; Yarovenko, H.; Vasilyeva, T. Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *J. Risk Financ. Manag.* **2022**, *15*, 613. https://doi.org/10.3390/jrfm15120613.
6. Kovacevic, A.; Radenkovic, S.D.; Nikolic, D. Artificial Intelligence and Cybersecurity in Banking Sector: Opportunities and Risks. *arXiv* **2024**, arXiv:2412.04495.
7. Jafri, J.A.; Mohd Amin, S.I.; Abdul Rahman, A.; Mohd Nor, S. A Systematic Literature Review of the Role of Trust and Security on Fintech Adoption in Banking. *Heliyon* **2023**, *10*, e22980. https://doi.org/10.1016/j.heliyon.2023.e22980.
8. Riasat, I.; Shah, M.; Gonul, M.S. Strengthening Cybersecurity Resilience: An Investigation of Customers' Adoption of Emerging Security Tools in Mobile Banking Apps. *Computers* **2025**, *14*, 129. https://doi.org/10.3390/computers14040129.
9. Al-Kumaim, N.H.; Alshamsi, S.K. Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *Appl. Sci.* **2023**, *13*, 5839. https://doi.org/10.3390/app13105839.
10. Căciulescu, A.R.; Rughiniș, R.; Țurcanu, D.; Radovici, A. Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy. *Risks* **2024**, *12*, 200. https://doi.org/10.3390/risks12120200.
11. Mishra, S. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Appl. Sci.* **2023**, *13*, 5875. https://doi.org/10.3390/app13105875.
12. Morshed, A.; Khrais, L.T. Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. *J. Risk Financ. Manag.* **2025**, *18*, 41. https://doi.org/10.3390/jrfm18010041.
13. Šijan, A.; Viduka, D.; Ilić, L.; Predić, B.; Karabašević, D. Modeling Cybersecurity Risk: The Integration of Decision Theory and Pivot Pairwise Relative Criteria Importance Assessment with Scale for Cybersecurity Threat Evaluation. *Electronics* **2024**, *13*, 4209. https://doi.org/10.3390/electronics13214209.
14. Si, S.-L.; You, X.-Y.; Liu, H.-C.; Zhang, P. DEMATEL Technique: A Systematic Review of the State-of-the-Art Literature on Methodologies and Applications. *Math. Probl. Eng.* **2018**, *2018*, 3696457. https://doi.org/10.1155/2018/3696457.
15. Taherdoost, H.; Madanchian, M. Multi-Criteria Decision Making (MCDM) Methods and Concepts. *Encyclopedia* **2023**, *3*, 77–87. https://doi.org/10.3390/encyclopedia3010006.
16. Dinu, I.A.; Nechita, R.-M.; Grecu, I.; Deselnicu, D.-C. Exploring Interconnections of Digital Marketing Risks: A Causal Modeling Approach. *Int. Conf. Manag. Ind. Eng.* **2025**, *12*, 145–153. https://doi.org/10.56177/12icmie2025.136.
17. Lu, M.-L.; Fan, P.-H. Applying DEMATEL to Discuss Key Factors in Shaping Organisational Culture of Lean Management. *S. Afr. J. Ind. Eng.* **2023**, *34*, 22–35. https://doi.org/10.7166/34-2-2884.
18. Deselnicu, D.C. *Risk Management*; Niculescu Publishing House: București, Romania, 2014.
19. Brutu, M.; Mihai, D. The Annual Employee Assessment Versus Their Remuneration—A Relationship Meant To Increase Business Competitiveness. *Sci. Bull.-Econ. Sci.* **2017**, *16*, 80–89.
20. Rodrigues, A.R.D.; Ferreira, F.A.F.; Teixeira, F.J.C.S.N.; Zopounidis, C. Artificial Intelligence, Digital Transformation and Cybersecurity in the Banking Sector: A Multi-Stakeholder Cognition-Driven Framework. *Res. Int. Bus. Financ.* **2022**, *60*, 101616. https://doi.org/10.1016/j.ribaf.2022.101616.
21. Jiang, E.X.; Yu, G.Y.; Zhang, J. Bank Competition Amid Digital Disruption: Implications for Financial Inclusion. *J. Financ.* **2026**, *81*, 1951–2004. https://doi.org/10.1111/jofi.70051.
22. Almi'ani, K.; Mirza, S.B.; Siyam, N.; Al-Jaziri, S.A.; Alqaryouti, O.; Zufferey, C. Global Adoption and Impact of Blockchain Technology in Government: Enhancing Transparency, Efficiency, and Trust in Public Services. *Information* **2026**, *17*, 235. https://doi.org/10.3390/info17030235.
23. Al-Afeef, M.A.; Alsmadi, A.A. The Future of Money: Blockchain as the Backbone of Secure and Transparent Finance. *Front. Blockchain* **2026**, *9*, 1792905. https://doi.org/10.3389/fbloc.2026.1792905.
24. Marotta, A.; Madnick, S. *Analyzing the Interplay Between Regulatory Compliance and Cybersecurity (Revised)*; Massachusetts Institute of Technology: Cambridge, MA, USA, 2020.

25. Sulong, Z.; Fuszder, M.H.R.; Abdullah, M.; Abakah, E.J.A. Cybersecurity Risk and Bank Risk-Taking. *J. Behav. Exp. Financ.* **2025**, *47*, 101080. https://doi.org/10.1016/j.jbef.2025.101080.
26. Le, P.; Nguyen, T.N. Banking Digital Drifts: What Are the Opportunities for Risk Assessment? In *The Future of Accounting and Finance: Embracing Technology, Digitalisation, Sustainability, Education, and Employability*; Trinh, V.Q., Pham, T.N., Eds.; Springer Nature : Cham, Switzerland, 2025; pp. 69–120.
27. PricewaterhouseCoopers. Evolution of Risk Management in Banking. Available online: https://www.pwc.com/m1/en/publications/evolution-of-risk-management-in-banking.html (accessed on 15 July 2026).
28. VALID Systems. Risk Management in Banking: Process and Best Practices. Available online: https://validadvantage.com/blog/risk-management-in-banking (accessed on 15 July 2026).
29. Deselnicu, D.C.; Barbu, A.; Haddad, S. Risk Management in a Logistics Company. In Proceedings of the 12th International Maritime Transport and Logistics Conference, Alexandria, Egypt, 12–14 March 2023; Volume 12, p. 14.
30. Betancourt, C.; Aranda, V.; García, C.; Villanueva, E. Strategic Risks and Financial Digitalization: Analyzing the Challenges and Opportunities for Fintech Firms and Neobanks. *J. Risk Financ. Manag.* **2026**, *19*, 66. https://doi.org/10.3390/jrfm19010066.
31. Bruno, E.; Pistolesi, F.; Teti, E. Cybersecurity Policy, ESG and Operational Risk: A Virtuous Relationship to Improve Banks' Performance. *Int. Rev. Econ. Financ.* **2025**, *99*, 104053. https://doi.org/10.1016/j.iref.2025.104053.
32. Chanda, R.C.; Vafaei-Zadeh, A.; Hanifah, H.; Nikbin, D. Assessing Cybersecurity Awareness among Bank Employees: A Multi-Stage Analytical Approach Using PLS-SEM, ANN, and fsQCA in a Developing Country Context. *Comput. Secur.* **2025**, *149*, 104208. https://doi.org/10.1016/j.cose.2024.104208.
33. Glaessner, T.; Kellermann, T.; McNevin, V. *Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues*; Policy Research Working Paper Series; The World Bank: Washington, DC, USA, 2002.
34. Burtescu, E. Principles of Minimum, Optimal and Imposed Financial Cyber Security. *Sci. Bull. Polytech. Univ. Buchar. Econ. Sci.* **2022**, *21*, 45–52.
35. Gâdoiu, M. Study on the Influence of Psychological Factors in Financial Decision Making. *Sci. Bull. Polytech. Univ. Buchar. Econ. Sci.* **2022**, *21*, 67–72.