



Development of a Human-AI Decision Intelligence Framework for Fraud Detection, Risk Analytics, and Operational Resilience in U.S. Digital Banking

Md Zafor Ikbal¹

[1]. Master of Science in Information Technology, Washington University of Science and Technology, VA, USA;
Email: zaforikbal29@gmail.com

Doi: [10.63125/7mhzkzj22](https://doi.org/10.63125/7mhzkzj22)

Received: 16 March 2026; Revised: 17 April 2026; Accepted: 08 May 2026; Published: 10 June 2026;

Abstract

The rapid expansion of artificial intelligence across U.S. digital banking has created a challenge concerning how automated analytical capability can be combined with human expertise to improve fraud detection, risk analytics, and operational resilience without weakening transparency, accountability, or decision quality. This study aimed to develop and empirically evaluate a Human-AI Decision Intelligence Framework that integrates technological intelligence, professional judgment, governance, and decision effectiveness within digitally intensive banking environments. A quantitative, cross-sectional, case-study-based design was employed using a structured five-point Likert-scale questionnaire administered to professionals representing commercial banks, digital banks, fintech organizations supporting banking, and payment or financial-technology service enterprises. Of 320 questionnaires distributed, 300 were returned and 292 usable responses were retained, producing a 91.3% usable response rate. The principal variables were Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance, Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience. Data analysis incorporated descriptive statistics, Cronbach's alpha reliability testing, Pearson correlation, multiple regression, ANOVA, and diagnostic assessment. AI-Enabled Fraud Detection Capability recorded the highest mean, $M = 4.15$, $SD = 0.57$, while Operational Resilience achieved $M = 4.10$, $SD = 0.58$. AI-Enabled Fraud Detection Capability strongly predicted Fraud Detection Effectiveness, $\beta = .39$, $p < .001$, and AI-Driven Risk Analytics Capability strongly predicted Risk Analytics Effectiveness, $\beta = .44$, $p < .001$. The integrated model explained 70.9% of the variance in Operational Resilience, $R = .842$, $R^2 = .709$, adjusted $R^2 = .703$, $F(6, 285) = 115.65$, $p < .001$, with Fraud Detection Effectiveness, $\beta = .28$, and Risk Analytics Effectiveness, $\beta = .25$, emerging as the strongest direct predictors. All eight hypotheses were supported. The findings imply that resilient digital banking depends on coordinated AI capabilities, human judgment, explainable governance, and effective fraud and risk decisions rather than automation alone.

Keywords

Human-AI Decision Intelligence; Fraud Detection; Risk Analytics; Operational Resilience; Digital Banking;

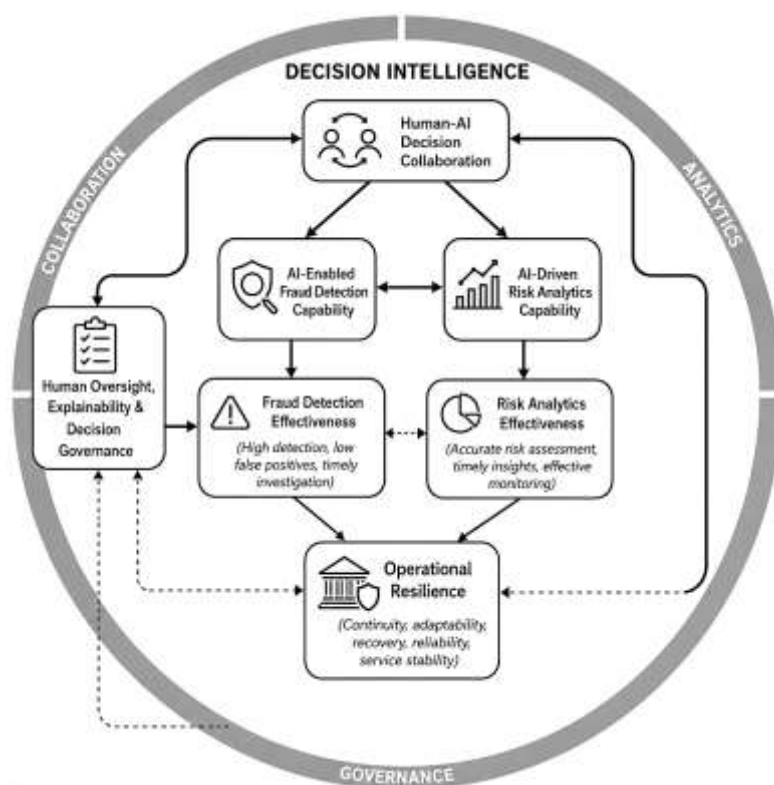
INTRODUCTION

Artificial intelligence, digital banking, and decision intelligence have become increasingly interconnected within contemporary financial services. Digital banking refers to the delivery, management, and execution of financial products, transactions, customer interactions, payments, lending services, and information through digitally enabled banking platforms rather than through predominantly physical and manually administered banking channels. Digital finance more broadly reflects the integration of financial activities with technological infrastructures, data-driven systems, digital platforms, and automated service mechanisms that reshape how financial institutions create, deliver, monitor, and control financial services (Gomber et al., 2018; Gomber et al., 2017). Financial technology has further transformed the architecture of banking by introducing technologically mediated payment systems, digital lending platforms, data-intensive credit assessment, automated financial intermediation, and algorithm-supported risk management processes (Thakor, 2020). Within this environment, artificial intelligence can be understood as a collection of computational approaches capable of performing analytical and cognitive functions such as pattern recognition, classification, prediction, anomaly identification, learning, and decision support. The increasing use of such capabilities in banking has created a need to understand not only the technical accuracy of AI models but also the way in which algorithmic outputs are combined with professional judgment and organizational decision processes. Human-AI Decision Intelligence can therefore be defined as an integrated decision architecture in which artificial intelligence provides computational scale, pattern recognition, prediction, and analytical support while human decision makers contribute contextual understanding, professional expertise, ethical judgment, accountability, and interpretation. This approach reflects the principle that human and machine capabilities can complement one another in organizational decision environments rather than being treated only as substitutes (Dellermann et al., 2019; Jarrahi, 2018). Organizational research has shown that AI-supported decisions may be structured through different combinations of human authority, algorithmic recommendations, sequential review, and joint decision arrangements, making the design of decision structures an important element of AI adoption (Shrestha et al., 2019). The international significance of this issue has increased with the globalization and digitization of banking services because financial institutions now process enormous volumes of transaction, customer, behavioral, credit, and operational data through interconnected platforms. In U.S. digital banking, these conditions are particularly important because banks, fintech firms, digital payment providers, card networks, and technologically enabled financial institutions must process high-speed transactions while simultaneously addressing fraud exposure, financial risk, regulatory obligations, customer protection, and service continuity. A Human-AI Decision Intelligence perspective consequently provides a suitable foundation for examining how algorithmic capabilities and human expertise can be combined within a banking environment in which both computational efficiency and accountable decision-making are essential (Jarrahi, 2018; Shrestha et al., 2019).

Human-AI Decision Collaboration represents one of the central components of decision intelligence because AI-supported banking systems do not operate independently from the professionals who interpret, verify, challenge, or act upon their outputs. Human-AI Decision Collaboration can be defined as a coordinated decision process in which human professionals and artificial intelligence systems contribute different forms of expertise to a shared analytical or operational task. In such arrangements, AI systems may identify patterns, rank risks, classify transactions, generate alerts, or recommend actions, while human decision makers assess contextual factors, resolve ambiguous cases, evaluate exceptional circumstances, and retain responsibility for decisions that require professional judgment. Research on human interaction with algorithms demonstrates that the acceptance of automated advice is influenced by more than technical accuracy. Individuals may reject algorithmic recommendations after observing errors even when algorithmic forecasts remain more accurate than human judgments, a phenomenon commonly described as algorithm aversion (Dietvorst et al., 2015). At the same time, willingness to use algorithms can increase when users are given some degree of control over their outputs, indicating that perceived human involvement can strengthen acceptance of automated decision support (Dietvorst et al., 2018). Other research has identified algorithm appreciation, whereby users sometimes assign greater weight to algorithmic recommendations than to comparable advice from human sources, demonstrating that human attitudes toward automation can vary substantially

across contexts and tasks (Logg et al., 2019). Trust therefore becomes an important component of Human-AI collaboration. Reliability, transparency, system behavior, and the way AI systems communicate their capabilities can influence whether users develop appropriate cognitive and emotional trust in automated systems (Glikson & Woolley, 2020). Effective collaboration must also distinguish between automation and augmentation. Automation transfers tasks or decision responsibilities from humans to technological systems, whereas augmentation combines machine capabilities with human expertise so that each contributes to the final decision process (Raisch & Krakowski, 2021). Explainability further affects this relationship because providing explanations does not automatically guarantee appropriate reliance. Users may over-trust incorrect AI recommendations or reject accurate recommendations when they fail to calibrate their trust effectively (Naiseh et al., 2021). Research on AI-supported decision processes also indicates that intermediate judgments made by users can shape subsequent trust and reliance behavior (Humr & Canan, 2024). In digital banking, these findings are directly relevant to transaction monitoring, fraud investigation, customer-risk assessment, credit evaluation, and operational-risk management because AI-generated alerts or scores acquire practical value only when they are interpreted and incorporated into appropriate decisions. Human-AI Decision Collaboration therefore involves a controlled interaction among machine-based analytical capability, human expertise, trust calibration, explanation, verification, and decision authority rather than unrestricted dependence on automated recommendations (Glikson & Woolley, 2020; Raisch & Krakowski, 2021).

Figure 1: Human-AI Decision Intelligence Framework for Fraud Detection, Risk Analytics, and Operational Resilience



Fraud detection represents one of the most established applications of artificial intelligence and computational analytics within banking and financial services. Financial fraud generally refers to intentional deceptive, unauthorized, or manipulative activity undertaken to obtain financial benefit, avoid financial obligations, or compromise legitimate financial processes, while fraud detection concerns the systematic identification of transactions, accounts, behaviors, or activities exhibiting characteristics associated with fraudulent conduct. Early studies demonstrated that computational intelligence could be used to recognize fraudulent credit-card behavior through techniques such as

support vector machines and artificial neural networks, establishing an analytical basis for machine-assisted fraud identification (Chen et al., 2005). Real-time fraud detection research further demonstrated the importance of examining customer spending behavior and transaction patterns as electronic commerce and digital payment activity expanded (Quah & Sriganesh, 2008). The wider field of financial fraud analytics subsequently developed through the application of classification, regression, clustering, prediction, outlier detection, visualization, and other data-mining approaches designed to distinguish legitimate activity from suspicious patterns (Ngai et al., 2011). Comparative empirical evidence has also shown that logistic regression, support vector machines, random forests, and related techniques can produce different levels of performance depending on transaction characteristics, sampling procedures, and the structure of available fraud data (Bhattacharyya et al., 2011). The importance of intelligent fraud detection has grown because purely manual review is costly, slow, and difficult to sustain in environments characterized by high transaction volumes and complex behavioral patterns (West & Bhattacharya, 2016). Fraud-detection systems additionally face methodological challenges such as extreme class imbalance, concept drift, large-scale data processing, delayed labels, and the need to identify suspicious activity rapidly enough to support meaningful intervention (Abdallah et al., 2016). Feature engineering also plays an important role because the effectiveness of fraud analytics depends not only on the selected algorithm but also on the representation of customer behavior, transaction aggregation, historical patterns, and the financial cost associated with classification errors (Bahnsen et al., 2016). Real-world fraud management frequently combines computational classification with manual investigation, illustrating the practical relevance of Human-AI collaboration in operational fraud processes (Carneiro et al., 2017). AI-Enabled Fraud Detection Capability can therefore be understood as an organizational capability encompassing real-time transaction monitoring, anomaly recognition, behavioral analytics, suspicious-pattern identification, automated alert generation, data preparation, and analyst-supported investigation. Within U.S. digital banking, such capability is particularly important because financial institutions must evaluate enormous volumes of transactions at high speed while limiting both undetected fraud and unnecessary restrictions placed on legitimate customers. Fraud detection is therefore not solely an algorithmic classification task but a decision process involving data, models, thresholds, analysts, investigative procedures, and organizational controls (Abdallah et al., 2016; Carneiro et al., 2017). The distinction between AI-enabled fraud-detection capability and actual fraud-detection effectiveness is necessary because technologically advanced systems do not automatically produce accurate and operationally useful decisions. Fraud Detection Effectiveness can be defined as the extent to which a banking fraud-management process successfully identifies suspicious behavior, minimizes missed fraud, controls false positives, enables timely investigation, supports accurate intervention, and reduces the operational burden associated with inappropriate alerts. Realistic fraud-detection environments are affected by extreme class imbalance because fraudulent transactions usually represent only a very small proportion of total activity, while legitimate transactions dominate available datasets. They are also influenced by changing fraud patterns, evolving customer behavior, delayed confirmation of fraudulent transactions, and continuously shifting transaction distributions (Dal Pozzolo et al., 2018). Such conditions create a nonstationary analytical environment in which models developed from historical data may not consistently identify every newly emerging form of suspicious behavior. Sequence-based modeling has demonstrated that transaction histories can provide useful behavioral information and that Long Short-Term Memory models can detect patterns that differ from those captured through static classification methods (Jurgovsky et al., 2018). However, strong statistical performance in experimental datasets cannot be assumed to translate directly into operational effectiveness. Research comparing academic fraud-detection methods with industry practice has identified gaps involving scalability, practical deployment, real-time processing, fraud investigation, evolving criminal strategies, and the usability of algorithmic outputs for professional reviewers (Ryman-Tubb et al., 2018). These concerns are particularly important when classifiers operate as opaque systems because fraud analysts often need to know why a transaction has been flagged, which behavioral characteristics influenced the alert, and whether contextual evidence supports escalation. Machine-learning studies in fintech applications have also demonstrated that the

effectiveness of fraud detection varies according to algorithm selection, feature representation, data characteristics, and the structure of financial activity being examined (Stojanović et al., 2021). In operational digital banking, a single transaction may move through several stages, including automated monitoring, anomaly scoring, behavioral comparison, threshold evaluation, fraud-alert generation, analyst examination, customer verification, escalation, and final authorization or blocking. The outcome is consequently affected by both computational and human components. AI may provide speed, scalability, and pattern recognition, while professional analysts provide contextual assessment, interpretation, exception handling, and decision accountability. This distinction supports the treatment of AI-Enabled Fraud Detection Capability and Fraud Detection Effectiveness as separate constructs within the present study. The first reflects the technological and analytical capacity of the banking institution, while the second represents the quality and effectiveness of fraud-related decisions generated through the broader Human-AI process (Dal Pozzolo et al., 2018; Ryman-Tubb et al., 2018). Risk analytics constitutes another major component of digital banking decision intelligence because financial institutions must continuously assess multiple forms of uncertainty extending beyond individual fraud events. Risk analytics refers to the systematic use of historical, transactional, financial, behavioral, operational, and contextual data to identify risk exposure, estimate probabilities, produce risk scores, recognize abnormal conditions, and support risk-control decisions. AI-Driven Risk Analytics Capability refers more specifically to the organizational ability to use artificial intelligence, machine learning, and advanced computational techniques for predictive risk assessment, behavioral risk scoring, early-warning detection, scenario analysis, customer-risk evaluation, and continuous monitoring of changing risk conditions. Digital banks operate within environments containing interconnected categories of credit risk, market risk, liquidity risk, operational risk, compliance risk, cybersecurity risk, and financial-crime risk, making effective analysis increasingly dependent on the capacity to process heterogeneous and high-volume datasets. Transaction-level information can strengthen financial risk assessment because behavioral and transactional variables may reveal changing borrower or customer conditions that conventional demographic and application-based variables cannot fully capture (Zhang et al., 2018).

Machine-learning applications have been documented across several areas of banking risk management, including credit, market, operational, and liquidity risk, illustrating the relevance of computational methods to risk detection, measurement, reporting, and management activities (Leo et al., 2019). Broader research on financial risk management has similarly shown that machine-learning techniques can support the modeling of complex nonlinear relationships and large data environments that may challenge conventional analytical approaches (Mashrur et al., 2020). AI and machine-learning methods have also been examined in credit-risk assessment, where data-driven models can support classification and prediction of borrower risk within increasingly digital financial ecosystems (Mhlanga, 2021). Predictive capability, however, does not eliminate the need for interpretation. Explainable machine-learning approaches in credit-risk management have demonstrated how predictive models can be supplemented with information concerning the factors that influence classifications or risk estimates, improving the interpretability of analytically generated decisions (Bussmann et al., 2021). This distinction makes it important to separate AI-Driven Risk Analytics Capability from Risk Analytics Effectiveness. The former represents an institution's technological ability to produce predictive and data-intensive assessments, while the latter reflects whether those assessments accurately identify risk, provide timely and meaningful information, strengthen professional judgment, and contribute to appropriate risk-control decisions. Within a Human-AI Decision Intelligence framework, algorithmic risk analytics can therefore serve as a scalable mechanism for identifying complex patterns, while human professionals evaluate contextual conditions, challenge questionable outputs, incorporate organizational knowledge, and determine the actions that should follow from the analytical evidence (Bussmann et al., 2021; Leo et al., 2019).

Human Oversight, Explainability, and Decision Governance form the control dimension of Human-AI Decision Intelligence because banking decisions involving fraud, risk, customers, and operational continuity require accountable mechanisms for interpreting and managing AI-generated outputs. Human oversight can be defined as the capacity of authorized professionals to observe, review,

challenge, modify, escalate, or override AI-supported recommendations according to clearly established responsibilities. Explainability refers to the extent to which the reasoning, influential factors, or analytical basis behind an AI-generated prediction or recommendation can be communicated in a form that relevant users can understand. Decision governance refers to the organizational rules, accountability structures, monitoring procedures, documentation requirements, validation mechanisms, escalation protocols, and control arrangements that determine how Human-AI decisions are produced and supervised. These dimensions are particularly relevant in banking because predictive accuracy alone is insufficient for a dependable decision architecture. Trust in AI is influenced by transparency, reliability, observable system behavior, and the ability of users to understand the role of automated systems within a decision process (Glikson & Woolley, 2020). Organizational structures also determine how decision authority is allocated between human actors and algorithms, including arrangements in which AI recommends and humans decide, humans provide input and algorithms decide, or both contribute sequentially to a final judgment (Shrestha et al., 2019).

Explainability must also be connected with trust calibration because an explanation can lead users to rely too heavily on an incorrect recommendation or to reject an accurate recommendation when the information is misunderstood (Naiseh et al., 2021). Financial risk-management research has demonstrated that explainable machine-learning techniques can make risk classifications more interpretable by identifying variables or conditions associated with particular predictions (Bussmann et al., 2021). Similar concerns arise in financial fraud detection because opaque classification models may provide limited investigative value when analysts cannot determine the reasons underlying suspicious-transaction alerts (Ryman-Tubb et al., 2018). Human oversight therefore should not be interpreted merely as the presence of an employee after an automated output has been produced. It represents the deliberate design of interaction among model outputs, professional expertise, validation requirements, escalation criteria, exception handling, and decision accountability. International financial-sector research has also linked digital operational resilience with information and communication technology risk, cybersecurity controls, third-party dependencies, governance, and supervisory arrangements, demonstrating that technological decision systems operate within broader structures of institutional control (Buttigieg & Brunelli Zimmermann, 2024). Within U.S. digital banking, Human Oversight, Explainability, and Decision Governance can consequently be treated as measurable capabilities that determine how effectively AI-generated fraud and risk information is interpreted, controlled, challenged, and translated into organizational decisions (Glikson & Woolley, 2020; Shrestha et al., 2019).

Operational resilience provides the central organizational outcome through which the combined effectiveness of Human-AI decision processes, fraud detection, and risk analytics can be examined. Operational resilience refers to the ability of an organization to maintain, adapt, restore, or recover critical operations when exposed to technological failures, fraud incidents, cyberattacks, process breakdowns, third-party disruptions, model failures, or other events that threaten service continuity. In financial institutions, the concept extends beyond conventional operational-risk management because it focuses not only on preventing adverse events but also on ensuring that important banking services continue to function or can be restored within acceptable conditions when disruptions occur. Operational resilience has therefore been described as an extension of operational-risk management centered on an institution's capacity to respond to and recover from disruptive events (Milkau, 2021). Financial institutions can also be viewed as complex adaptive systems whose resilience depends on their ability to absorb shocks, adjust internal processes, coordinate resources, and recover from disturbances affecting interconnected operational functions (Butler & Brooks, 2021). The increasing dependence of financial institutions on digital technologies has strengthened the connection among resilience, cybersecurity, technology governance, information and communication technology risk, and third-party service dependencies (Buttigieg & Brunelli Zimmermann, 2024). These dimensions are closely associated with fraud and risk analytics because operational disruptions can arise not only from technical infrastructure failures but also from undetected fraudulent transactions, compromised accounts, inappropriate automated decisions, inaccurate risk classifications, excessive false-positive

alerts, delayed investigations, or inadequate escalation of emerging threats. The digital transformation of financial services has intensified these relationships by increasing the degree to which payments, customer interactions, lending decisions, risk assessments, and operational processes depend on interconnected technological platforms (Gomber et al., 2017; Thakor, 2020). Within this environment, operational resilience is partly determined by the quality and speed of decisions through which abnormal transactions, financial risks, and operational threats are detected, interpreted, escalated, and controlled. Existing research has frequently examined these dimensions through separate streams. Fraud-detection studies have focused heavily on classification algorithms and detection accuracy, risk-management studies have concentrated on predictive assessment and machine learning, Human-AI research has examined trust, augmentation, algorithm acceptance, and decision structures, while resilience research has emphasized continuity, adaptation, and recovery. The present quantitative, cross-sectional, case-study-based study integrates these domains by examining Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, and Human Oversight, Explainability, and Decision Governance in relation to Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience in U.S. digital banking. The relationships among these variables provide the analytical foundation for testing how Human-AI decision capabilities are associated with fraud-management performance, risk-analysis performance, and resilient digital banking operations (Butler & Brooks, 2021; Milkau, 2021).

Background of the Study

The rapid digitalization of banking has transformed the way financial institutions process transactions, evaluate customer behavior, manage financial risks, detect fraudulent activity, and maintain continuity of essential services. In the United States, digital banking environments now depend heavily on interconnected information systems, mobile applications, online platforms, automated transaction-processing infrastructures, cloud-based services, analytical technologies, and artificial intelligence tools that generate large volumes of data and support increasingly complex decisions. This transformation has created substantial opportunities for financial institutions to improve speed, accuracy, scalability, and responsiveness, while it has also increased the complexity of fraud exposure, technology-related risk, cybersecurity threats, operational disruptions, and data-intensive decision-making. Conventional fraud-detection and risk-management approaches that depend heavily on static rules or manual review may be insufficient when institutions must evaluate millions of transactions, detect rapidly changing behavioral patterns, and distinguish legitimate activity from increasingly sophisticated fraudulent behavior. Artificial intelligence and machine-learning systems provide advanced capabilities for identifying anomalies, recognizing hidden patterns, generating risk scores, predicting suspicious behavior, and supporting real-time decision-making. However, banking decisions cannot be treated solely as technical classification problems because many fraud and risk situations require contextual interpretation, professional judgment, regulatory understanding, accountability, and evaluation of circumstances that may not be fully represented within algorithmic models. The concept of Human-AI Decision Intelligence therefore provides an appropriate basis for combining computational capabilities with human expertise in a structured decision environment. Under this approach, AI supports data processing, prediction, classification, and analytical reasoning, while banking professionals provide interpretation, verification, escalation, exception handling, and final judgment where necessary. Fraud detection effectiveness and risk analytics effectiveness consequently depend not only on the availability of advanced AI technologies but also on how effectively those technologies are integrated with human decision processes, explainability mechanisms, oversight structures, and decision governance. These combined capabilities are also closely connected with operational resilience because a bank must be able to detect abnormal conditions, make timely risk decisions, respond to fraud-related events, maintain critical services, and recover from disruptions. The present study has therefore been developed around the need to examine Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance as interconnected dimensions that may strengthen Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience within U.S. digital banking.

Problem Statement

The increasing dependence of U.S. digital banking institutions on artificial intelligence has created a critical decision-management problem concerning how automated analytical capabilities should be combined with human expertise to achieve effective fraud detection, accurate risk analytics, and resilient banking operations. Digital banking institutions process large volumes of transactions and customer interactions through automated systems, creating an environment in which fraud attempts, account compromises, behavioral anomalies, financial risks, and operational threats must often be detected and evaluated within very limited timeframes. Artificial intelligence can process these data at a scale that is impossible for human analysts to reproduce manually, yet automated systems may generate false-positive alerts, fail to identify unfamiliar fraud patterns, provide insufficiently transparent recommendations, or produce outputs that require professional interpretation before action is taken. Excessive reliance on automation can therefore create decision risks, while excessive dependence on manual review can reduce speed, scalability, and consistency. A further problem concerns the fragmentation of existing banking decision processes. Fraud detection, risk analytics, AI governance, human oversight, and operational resilience are frequently managed as related but organizationally separate functions. This separation may limit the ability of institutions to understand how improvements in one capability contribute to performance in another. For example, a highly sophisticated fraud-detection algorithm may not improve organizational performance if analysts do not trust or understand its alerts, while advanced predictive risk analytics may have limited value if decision-makers cannot convert risk information into timely and appropriate operational actions. Similarly, explainability and governance mechanisms may enhance accountability, but their contribution cannot be fully understood without examining their relationships with decision effectiveness. The principal research problem is therefore the absence of an integrated and empirically tested framework that explains how Human-AI collaboration, AI-enabled fraud detection, AI-driven risk analytics, and human-centered governance collectively contribute to effective fraud and risk decisions and ultimately to operational resilience in U.S. digital banking. This problem is particularly important because operational resilience depends on an institution's capacity to recognize threats, interpret complex information, make effective decisions, maintain critical services, and recover from disruptive conditions. The study addresses this problem by developing and quantitatively testing a Human-AI Decision Intelligence Framework that integrates technological capability, human judgment, analytical effectiveness, governance, and resilience within a single explanatory model.

Objectives of the Study

The principal purpose of this study is to develop and empirically evaluate a Human-AI Decision Intelligence Framework for Fraud Detection, Risk Analytics, and Operational Resilience in U.S. Digital Banking through a quantitative, cross-sectional, case-study-based research design. The study is intended to determine whether the integration of human expertise and AI-supported analytical capabilities can provide a coherent explanation of fraud-detection performance, risk-analysis performance, and organizational resilience within digitally intensive banking environments. More specifically, the first objective is to examine the extent to which Human-AI Decision Collaboration influences Fraud Detection Effectiveness by assessing whether collaboration between automated systems and professional banking personnel improves the identification, interpretation, and management of potentially fraudulent activities. The second objective is to determine the influence of AI-Enabled Fraud Detection Capability on Fraud Detection Effectiveness, with emphasis on real-time transaction monitoring, anomaly identification, behavioral analysis, automated alerts, and pattern-recognition capabilities. The third objective is to evaluate the relationship between AI-Driven Risk Analytics Capability and Risk Analytics Effectiveness by examining the role of predictive assessment, risk scoring, early-warning information, and data-supported risk identification. The fourth objective is to assess the contribution of Human Oversight, Explainability, and Decision Governance to both fraud detection and risk analytics, recognizing that technologically generated outputs must operate within transparent, accountable, and professionally controlled decision environments. The fifth objective is to determine whether Fraud Detection Effectiveness contributes significantly to Operational Resilience by improving the institution's ability to recognize and respond to fraudulent disruptions while protecting

essential banking services. The sixth objective is to examine the effect of Risk Analytics Effectiveness on Operational Resilience by determining whether accurate and timely risk information strengthens organizational preparedness, response, and continuity. The seventh and overarching objective is to determine whether the principal Human-AI Decision Intelligence capabilities jointly explain a significant proportion of operational resilience within U.S. digital banking. Through these objectives, the study establishes a measurable connection among technological capability, human judgment, analytical effectiveness, and resilient organizational performance and provides a structured foundation for testing the proposed relationships through descriptive statistics, reliability analysis, Pearson correlation, and multiple regression modeling.

Research Hypotheses

The research hypotheses have been formulated to statistically evaluate the relationships proposed within the Human-AI Decision Intelligence Framework and to determine whether the selected technological, human, and analytical capabilities make significant contributions to fraud detection, risk analytics, and operational resilience in U.S. digital banking. The first hypothesis, H1, proposes that Human-AI Decision Collaboration has a significant positive effect on Fraud Detection Effectiveness, based on the expectation that combining machine-based analytical capabilities with professional judgment can improve fraud-related decision performance. The second hypothesis, H2, proposes that AI-Enabled Fraud Detection Capability has a significant positive effect on Fraud Detection Effectiveness because stronger automated monitoring, anomaly identification, behavioral analysis, and pattern-recognition capabilities are expected to strengthen the detection of suspicious financial activity. The third hypothesis, H3, proposes that AI-Driven Risk Analytics Capability has a significant positive effect on Risk Analytics Effectiveness, reflecting the expectation that predictive modeling, risk scoring, and data-driven early-warning capabilities improve the quality and timeliness of banking risk assessments. The fourth hypothesis, H4, states that Human Oversight, Explainability, and Decision Governance have a significant positive effect on Fraud Detection Effectiveness because transparent and accountable decision processes may strengthen the interpretation and management of AI-generated fraud alerts. The fifth hypothesis, H5, proposes that Human Oversight, Explainability, and Decision Governance have a significant positive effect on Risk Analytics Effectiveness by supporting appropriate interpretation, review, validation, and use of AI-generated risk information. The sixth hypothesis, H6, proposes that Fraud Detection Effectiveness has a significant positive effect on Operational Resilience because effective fraud identification and response can reduce disruption and support continuity of banking services. The seventh hypothesis, H7, states that Risk Analytics Effectiveness has a significant positive effect on Operational Resilience because accurate risk identification and timely analytical information can improve organizational preparedness and response. Finally, H8 proposes that Human-AI Decision Intelligence capabilities jointly have a significant positive effect on Operational Resilience. These eight hypotheses create the statistical structure for the study and will be tested using correlation and regression analyses to determine the direction, strength, significance, and explanatory power of the relationships among the principal variables.

Significance of the Research

i. Academic significance: This research is significant because it integrates several research domains that are often examined separately, including Human-AI collaboration, artificial intelligence, fraud detection, predictive risk analytics, explainability, decision governance, and operational resilience. By incorporating these dimensions into one quantitative framework, the study provides a more comprehensive basis for understanding AI-supported decision-making within digital banking rather than examining individual technologies or banking functions independently.

ii. Theoretical significance: The research provides an opportunity to interpret digital banking decision capabilities through a coherent theoretical perspective in which organizations develop technological and human capabilities for sensing threats, making effective decisions, adapting operational processes, and maintaining resilient performance. The integration of Human-AI decision mechanisms with fraud and risk outcomes strengthens the theoretical connection between digital capability and organizational resilience.

iii. Banking-management significance: The findings can provide banking managers with evidence regarding which Human-AI capabilities are most strongly associated with effective fraud detection, risk analytics, and operational resilience. This is important because institutions may invest heavily in AI technologies without understanding whether technological capability alone is sufficient or whether human collaboration, explainability, and governance are equally important determinants of performance.

iv. Fraud-management significance: The study is significant to fraud analysts and financial-crime professionals because it evaluates fraud detection as a combined technological and human decision process. This approach recognizes that successful fraud management depends on more than generating automated alerts and includes the interpretation, verification, escalation, and management of suspicious activities.

v. Risk-management significance: The research provides value to risk-management professionals by examining whether AI-driven risk analytics improves the effectiveness of risk assessment and whether stronger risk analytics contributes to operational resilience. This creates a direct link between predictive analytical capability and broader organizational performance.

vi. AI governance significance: The inclusion of Human Oversight, Explainability, and Decision Governance makes the study relevant to organizations seeking to establish transparent and accountable AI-supported decision systems. It provides a measurable way of examining whether governance-oriented capabilities are associated with improved banking decisions.

vii. Operational resilience significance: The research is important because it places operational resilience as the principal organizational outcome, allowing fraud detection and risk analytics to be examined in relation to the bank's capacity to maintain, adapt, and recover critical digital services during disruptive conditions.

LITERATURE REVIEW

The literature surrounding Human-AI Decision Intelligence in digital banking extends across several closely connected fields, including artificial intelligence, financial technology, fraud detection, banking risk analytics, explainable AI, organizational decision-making, human oversight, and operational resilience. These areas have developed from different disciplinary perspectives, yet they increasingly intersect within digital banking environments where institutions must process large volumes of financial information, identify suspicious behavior, assess uncertainty, respond to operational threats, and make accountable decisions under conditions of speed and complexity. Research on AI and digital finance has established the growing importance of machine learning, automated classification, predictive modeling, and data-intensive decision support in financial services, while fraud-detection studies have concentrated on the identification of anomalous or suspicious transactions through statistical and computational methods. A related body of research has examined the use of advanced analytics for credit, operational, market, and transaction-related risk assessment. At the same time, Human-AI research has emphasized that technological capability alone does not determine decision quality because human trust, professional judgment, transparency, interpretability, and appropriate allocation of decision authority influence whether AI-generated outputs are accepted and effectively applied. These concerns are particularly relevant in banking because errors in fraud detection or risk assessment can affect customers, financial losses, regulatory compliance, operational stability, and institutional reputation. Operational resilience research provides an additional dimension by focusing on the capacity of financial institutions to sustain essential services, respond to disruptive events, adapt operational processes, and recover critical functions. The present literature review therefore organizes the existing knowledge into six interconnected areas that correspond directly to the proposed research model. These areas include Human-AI Decision Intelligence and collaborative decision-making in digital banking, AI-enabled fraud detection, AI-driven risk analytics together with explainability and governance, operational resilience in U.S. digital banking, the theoretical foundation of the study, and the conceptual framework integrating the principal constructs. This structure enables the literature to be examined systematically while establishing the relationships among technological capability, human decision processes, analytical effectiveness, and resilient banking operations.

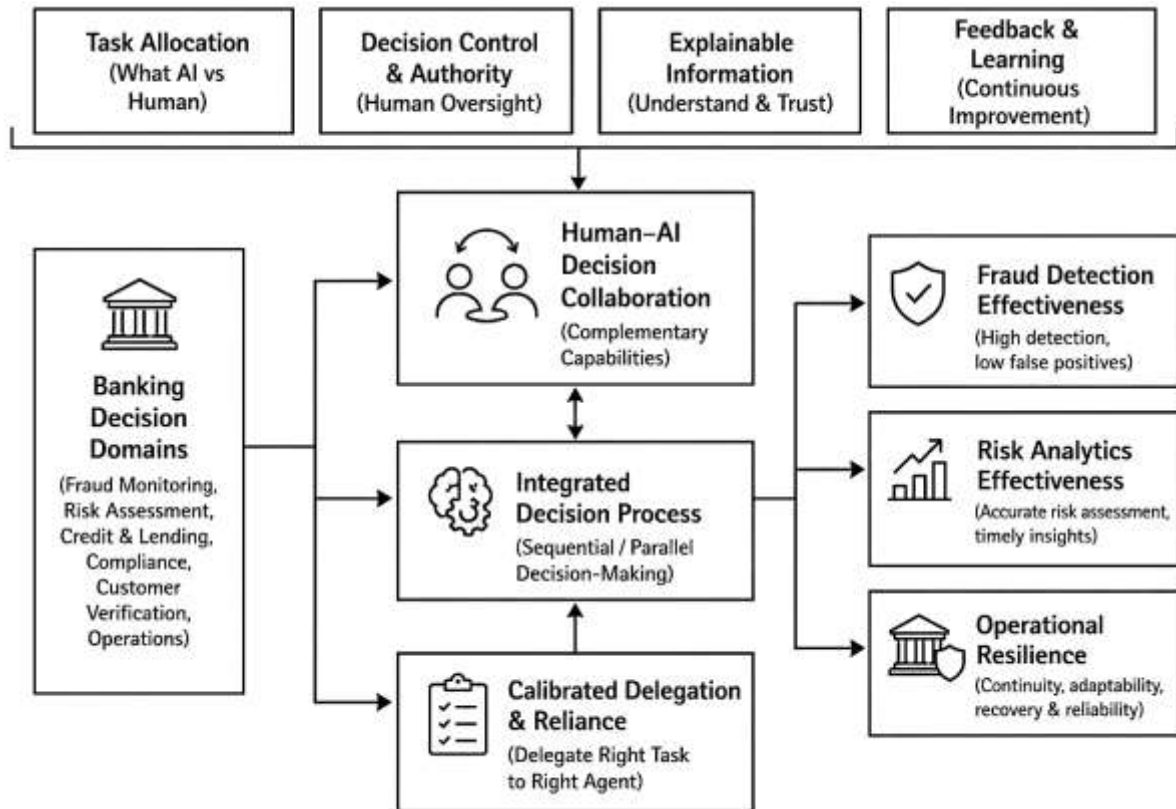
Human-AI Decision Intelligence and Collaborative Decision-Making in Digital Banking

Human-AI Decision Intelligence in digital banking refers to the structured integration of human judgment, organizational knowledge, and artificial intelligence capabilities within financial decision processes that require speed, consistency, contextual understanding, and accountability. In digital banking environments, decisions concerning transaction monitoring, fraud alerts, customer verification, credit assessment, risk classification, compliance review, and operational escalation are increasingly supported by machine-learning models capable of processing large and complex datasets beyond unaided human capacity. Human decision makers remain important because they interpret unusual cases, incorporate contextual information, evaluate exceptions, and determine actions when model outputs are uncertain or when decisions carry material consequences. Human-AI collaboration should therefore be understood as an organizational arrangement rather than a simple interaction between a user and a software tool. Its design determines which tasks are assigned to algorithms, which remain under human control, how outputs are combined, and how feedback is incorporated into subsequent decisions. Human and AI agents may operate sequentially, where one produces information that the other reviews, or in parallel, where both produce judgments that are integrated. The effectiveness of either configuration depends on task allocation, communication, exception handling, and learning. Organizational design research has emphasized that Human-AI collaborative decision-making involves division of labor, task interdependence, specialization, and learning configurations that can determine whether combined performance exceeds individual performance ([Puranam, 2021](#)). Algorithm-supported decision systems also require careful attention to final decision authority. When algorithms generate predictions or risk assessments while humans retain final judgment, decision-making becomes sociotechnical because analytical outputs interact with human interpretation, institutional rules, and professional discretion. Research on algorithm-in-the-loop decision-making has shown that providing algorithmic advice does not automatically improve human decisions and that the structure through which recommendations are received and used can materially shape outcomes ([Green & Chen, 2019](#)). These considerations are particularly relevant to digital banking because fraud and risk decisions frequently require computational screening together with accountable human review.

The quality of Human-AI Decision Intelligence also depends on whether people can determine when to rely on AI, when to challenge it, and when a task should remain under human judgment. Digital banking decisions often involve heterogeneous cases, incomplete information, changing transaction patterns, and varying levels of risk, making uniform allocation of decision authority unsuitable. A fraud model may identify common anomalous patterns effectively while struggling with rare contextual situations, whereas an experienced analyst may recognize unusual circumstances but cannot continuously evaluate the same transaction volume or number of variables as an automated system. Productive collaboration therefore requires an allocation mechanism that matches decision tasks with the capabilities of the most suitable agent. Experimental evidence has shown that Human-AI teams can outperform either humans or AI working independently under appropriate delegation structures, while human decision makers may perform poorly when they inaccurately assess their own competence and delegate unsuitable tasks to AI. This limitation has been associated with insufficient metaknowledge about personal capabilities rather than simple unwillingness to use algorithms ([Fügener et al., 2022](#)). Such findings are particularly relevant to banking because analysts must evaluate both an AI recommendation and the conditions under which the model is likely to be reliable. Decision control is therefore another important component of collaboration. Users who retain meaningful authority to review or modify AI-supported recommendations may engage more effectively with the system and maintain a clearer understanding of their responsibility within the decision process. Experimental research has found that decision control can improve user perceptions, understanding, trust, and compliance with AI recommendations, while explanations may increase cognitive complexity when they are not designed according to the user's capacity to process them ([Westphal et al., 2023](#)). In digital banking, explainability therefore needs to be integrated with workflow design. Fraud analysts and risk professionals require information that clarifies why an alert or score has been generated without creating unnecessary cognitive burden. Human-AI Decision Collaboration consequently requires calibrated reliance, appropriate delegation, decision control, and interpretable

information so that automated recommendations strengthen professional reasoning. These elements support a banking environment in which AI performs data-intensive analytical tasks while humans validate, contextualize, challenge, and govern consequential actions.

Figure 2: Human-AI Collaborative Decision-Making Framework for Digital Banking Effectiveness and Operational Resilience



Within financial services, the relevance of Human-AI Decision Intelligence becomes especially visible when automated analytics are integrated with expert judgment in lending, underwriting, fraud investigation, customer assessment, and risk management. Financial decisions combine structured variables, historical records, behavioral indicators, policy requirements, risk measures, and case-specific information, creating conditions in which neither fully manual nor fully automated decision-making is universally appropriate. AI systems can provide consistent analytical treatment of large datasets and identify patterns that may be difficult for human decision makers to detect, while banking professionals can evaluate contextual circumstances, assess unusual cases, apply institutional knowledge, and assume responsibility for decisions requiring interpretation. This complementary structure is particularly relevant to the present research because Human-AI Decision Collaboration is expected to influence how effectively AI-enabled fraud detection and AI-driven risk analytics are converted into operational decisions. Direct evidence from financial underwriting has shown that combining human expertise with AI can reduce decision noise and support augmented decision-support systems rather than treating automation as a complete replacement for professional underwriters. The same research identified the relevance of explainable lending rules, consistency analysis, and the management of variability in human judgments when collaborative financial decision processes are designed (Sachan et al., 2024). This evidence provides a direct financial-services basis for treating Human-AI collaboration as an organizational capability measurable through joint decision-making, human verification of AI outputs, appropriate intervention in uncertain cases, and effective use of algorithmic recommendations. In U.S. digital banking, these collaborative mechanisms can operate across fraud-monitoring teams, financial-crime units, risk departments, digital operations, customer authentication processes, lending functions, and other areas in which model-generated

information must be translated into timely action. The central issue is not whether humans or AI should dominate financial decision-making, but whether institutional processes allocate analytical and judgmental responsibilities in a manner that supports consistent, transparent, and accountable decisions. Human-AI Decision Intelligence therefore provides a basis for examining technological analysis and professional judgment as interdependent components of banking decision performance. When connected with fraud detection effectiveness, risk analytics effectiveness, and operational resilience, Human-AI collaboration becomes a measurable organizational capability through which digital banks identify threats, interpret risk information, verify analytical recommendations, authorize interventions, and coordinate responses across technology-intensive banking operations.

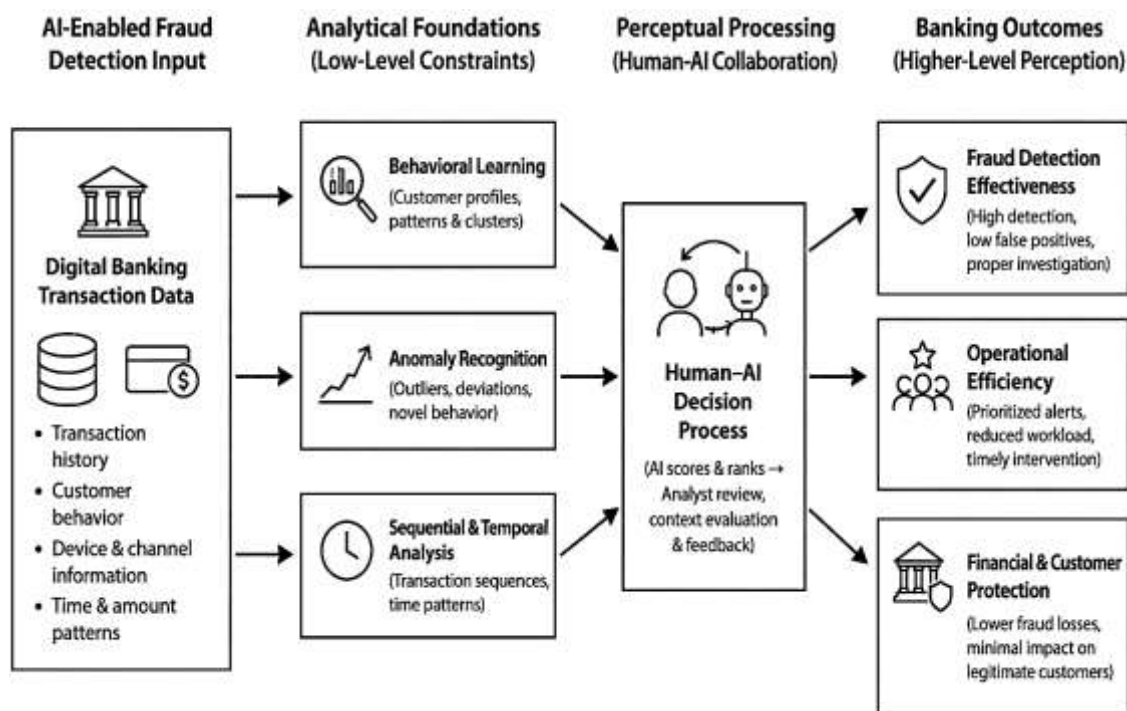
AI-Enabled Fraud Detection in Digital Banking

Artificial intelligence has become a central analytical capability in digital fraud detection because banking transactions are generated at a speed, volume, and complexity that make continuous manual screening impractical. AI-enabled fraud detection can be understood as the use of machine-learning, neural-network, anomaly-detection, and behavioral-profiling techniques to identify transactions or customer activities that depart from legitimate patterns and therefore require automated intervention or professional investigation. Within digital banking, the analytical problem is not limited to identifying a stolen card or a single unauthorized payment. Fraud may involve account takeover, credential theft, transaction manipulation, abnormal transfers, coordinated payment activity, phishing-related compromise, or repeated actions designed to remain below predefined monitoring thresholds. Effective AI systems consequently depend on behavioral information derived from historical transactions, customer profiles, transaction frequency, monetary values, time patterns, and relationships among successive activities. A particularly relevant contribution to online banking fraud research was BankSealer, a decision-support system that combined local customer profiles, global customer clusters, and temporal anomaly analysis to rank suspicious transactions while providing information that analysts could interpret during investigation ([Carminati et al., 2015](#)). This approach is important to the present study because it demonstrates that digital fraud detection can operate as a Human-AI decision process rather than as a completely autonomous classification mechanism. The AI component can continuously compare incoming behavior with learned patterns and prioritize cases according to anomaly or risk, whereas human investigators can evaluate contextual circumstances, validate unusual activity, and determine appropriate actions. Such integration is relevant in U.S. digital banking, where institutions must process large transaction volumes while reducing financial losses and unnecessary interference with legitimate customers. AI-Enabled Fraud Detection Capability therefore represents more than possession of a machine-learning model. It includes an institution's ability to collect relevant transaction data, construct behavioral representations, recognize anomalies, generate timely alerts, rank suspicious cases, and provide analytical evidence that can be incorporated into a controlled fraud-management workflow.

The effectiveness of AI-enabled fraud detection also depends heavily on how classification models are designed and evaluated. Fraud datasets are characteristically imbalanced because legitimate transactions greatly outnumber fraudulent cases, and a model that maximizes overall accuracy can therefore appear successful while failing to identify a meaningful proportion of actual fraud. This creates a need for analytical methods that consider minority-class recognition, false-positive costs, false-negative costs, transaction values, and the operational burden created by unnecessary investigations. Research using a customized Bayesian Network Classifier demonstrated that fraud-detection models can be optimized not only for conventional classification performance but also for economic efficiency, showing that the most statistically favorable model is not necessarily the model that produces the greatest financial value for a payment organization ([de Sá et al., 2018](#)). This distinction is important in digital banking because false negatives can permit fraudulent losses, while false positives can produce blocked legitimate transactions, customer dissatisfaction, additional analyst workload, and avoidable operational costs. Neural-network research has also demonstrated the feasibility of end-to-end fraud scoring on very large real-world card-payment datasets, illustrating how deep-learning architectures can generate transaction-level fraud scores from large-scale banking data ([Gómez et al., 2018](#)). These studies support a broader interpretation of AI-Enabled Fraud Detection Capability as the capacity to

transform high-volume transaction data into risk-sensitive and operationally usable classifications. Model performance should therefore be evaluated through measures suited to imbalanced classification and banking priorities rather than accuracy alone. Precision, recall, sensitivity, false-positive rates, area-under-curve measures, and economically weighted criteria provide different views of practical fraud-detection performance. In a Human-AI Decision Intelligence environment, these outputs also influence how investigators allocate attention because high-risk cases may require immediate review while low-risk cases may be processed automatically. Fraud-detection quality consequently depends on the interaction among algorithmic discrimination, alert prioritization, business costs, and analyst capacity, which supports the distinction between AI-Enabled Fraud Detection Capability and Fraud Detection Effectiveness in the present study.

Figure 3: AI-Enabled Fraud Detection and Human-AI Decision Framework in Digital Banking



A further challenge for AI-enabled fraud detection is that fraudulent behavior and legitimate customer behavior are not static. Fraudsters modify strategies in response to controls, customer purchasing patterns change over time, and new transaction channels may generate behaviors that were not represented in earlier training data. A fraud-detection architecture must therefore address novelty, concept drift, limited labels, and the possibility that emerging fraud patterns differ from previously confirmed cases. Hybrid learning approaches provide one response to this problem. Research combining unsupervised and supervised learning has shown that anomaly or outlier information can complement classifiers trained on labeled fraud cases, allowing detection systems to benefit from both known fraud patterns and unusual behavior that does not closely resemble historical examples (Carcillo et al., 2021). This combination is highly relevant to digital banking because supervised models are strongest when historical labels reliably represent the phenomenon being classified, whereas unsupervised methods can identify deviations deserving investigation even when a confirmed fraud label is unavailable. Deep sequential approaches provide another mechanism for representing changing transactional behavior because fraud may be embedded within sequences rather than isolated transactions. An ensemble of deep sequential models demonstrated that recurrent neural-network architectures can be combined to improve credit-card fraud detection by learning temporal patterns across transaction sequences and aggregating the strengths of multiple models (Forough & Momtazi, 2021). From the perspective of the present research, these developments show that AI-Enabled Fraud Detection Capability should include adaptability, behavioral learning, sequential analysis, ensemble

reasoning, and support for investigation under uncertainty. They also reinforce the role of human analysts because changing fraud environments create cases in which historical models may provide incomplete guidance. Analysts can contribute domain knowledge, interpret novel scenarios, review uncertain classifications, and provide feedback for model refinement. Within U.S. digital banking, AI-enabled fraud detection can therefore be understood as an integrated decision capability in which transaction intelligence, anomaly recognition, predictive scoring, model adaptation, and human investigation operate together to support Fraud Detection Effectiveness.

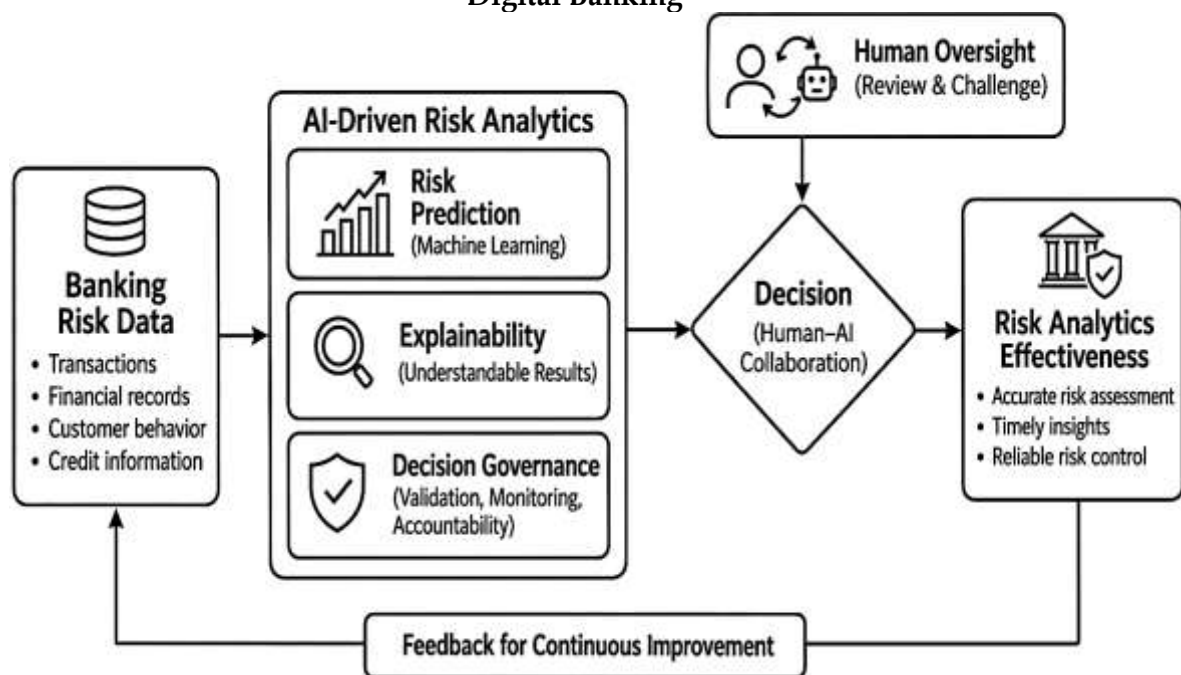
AI-Driven Risk Analytics, Explainability, and Decision Governance

AI-driven risk analytics has become an important component of digital banking because financial institutions must evaluate credit exposure, transaction uncertainty, customer behavior, operational vulnerabilities, and changing risk conditions across large datasets (Debasish, 2021; Md. Abdur & Iftekhar, 2021). AI-driven risk analytics can be defined as the systematic use of machine-learning and computational methods to identify risk patterns, estimate probabilities of adverse outcomes, classify customers or transactions according to risk, and provide timely analytical information for professional decision-making (Md Ashfaq & Abdullah Mohammad, 2022; Md Asif Ali Sheak & Risha, 2022). Traditional risk models commonly rely on predefined statistical relationships and selected financial variables, whereas machine-learning approaches can process larger numbers of variables and represent nonlinear interactions that may be difficult to capture through conventional scoring procedures (Mohammad Abir Chowdhury & Tonay, 2022; Nishat & Mst Kaniz, 2022). Consumer-credit research has demonstrated that transaction records, credit-bureau information, account balances, and behavioral data can be combined through machine-learning algorithms to generate useful forecasts of delinquency and default risk. Such models can identify subtle relationships in large banking datasets and produce frequently updated assessments that respond to changes in customer financial behavior (Khandani et al., 2010). In digital banking, this capability is relevant to lending, customer-risk classification, transaction-risk assessment, financial-crime monitoring, and operational decision support because banking risks are often reflected in combinations of behavioral and financial indicators (Abdullah Mohammad, 2023; Shaiful et al., 2022). The selection of analytical techniques also matters because alternative classifiers can differ in predictive performance and managerial usefulness. Large-scale benchmarking of credit-scoring algorithms has shown that no single classification method should automatically be assumed to dominate across all datasets and evaluation measures, and that assessment should consider predictive accuracy together with practical consequences (Lessmann et al., 2015). For U.S. digital banking, AI-Driven Risk Analytics Capability should therefore be treated as an organizational capability involving data integration, model selection, predictive assessment, performance evaluation, and timely delivery of risk information rather than the mere possession of an advanced algorithm (Mohammad Abir Chowdhury, 2023; Mohammad Badrul & Md. Mominul, 2023). Its value depends on whether diverse banking data can be transformed into reliable and actionable evidence for risk decisions.

The increasing analytical power of machine-learning models also creates an interpretability problem because highly predictive systems may produce outputs that are difficult for banking professionals to understand, evaluate, or challenge (Ashrafuzzaman, 2024; Muhammad Zahidul, 2023). Explainability refers to the ability of an AI system to provide information about how a prediction, classification, risk score, or recommendation has been generated, while interpretability concerns the extent to which a human user can understand the relationship between model inputs and outputs (Kazi Rakib Hasan, 2024; Md Anisur Rahman, 2024). These properties are important in digital banking because risk decisions can affect lending, transaction approval, account restrictions, fraud investigation, customer treatment, compliance, and operational escalation. A model that provides an accurate risk score but insufficient information about its basis can create difficulties for analysts who must determine whether the output is reasonable in a specific case. Explainable Artificial Intelligence has therefore developed as a field concerned with methods that make AI behavior more understandable to users and stakeholders (Md Asif Ali Sheak, 2024; Nishat & Jahanara, 2024). A major synthesis of XAI research has connected explainability with transparency, trustworthiness, causality, informativeness, confidence, fairness, and usability, indicating that explanations should be designed around the needs of the people

who must use them (Barredo Arrieta et al., 2020). In banking, an explanation may identify which transaction characteristics, account behaviors, financial variables, or historical patterns contributed most strongly to a risk classification, allowing analysts to compare model outputs with contextual information (Debasish, 2025; Tonay et al., 2024). Explainability, however, should not be treated as a complete solution for opaque systems. In high-stakes decisions, post hoc explanations of black-box models may create an appearance of understanding without faithfully representing the model's actual reasoning (Jannatul, 2025; Md Anisur Rahman, 2025). Research has therefore argued that inherently interpretable models should be preferred in many high-stakes settings when comparable performance can be obtained, because direct interpretability provides stronger grounds for scrutiny than explanations produced after a black-box prediction (Rudin, 2019). Within Human-AI Decision Intelligence, explainability consequently operates as a bridge between computational risk assessment and professional judgment by making analytical outputs available for review, challenge, validation, and responsible action (Md Arif Uz et al., 2025; Md Mahamud Pervaz, 2025).

Figure 4: AI-Driven Risk Analytics, Explainability, and Decision Governance Framework in Digital Banking



Decision governance extends the Human-AI framework beyond prediction and explanation by defining how responsibility, monitoring, documentation, validation, escalation, and accountability are organized throughout the lifecycle of AI-supported banking decisions (Mohammad Abir Chowdhury, 2025; Mohammad Badrul, 2025). In digital banking, decision governance can be understood as the institutional structures and procedures that determine who may develop, approve, deploy, monitor, challenge, modify, or override analytical systems and how evidence concerning model performance is documented and reviewed (Nishat, 2025; Nuzhat Sadia, 2025). This dimension is essential because AI-driven risk analytics can influence lending, fraud management, customer monitoring, compliance, financial-crime control, and operational-risk management, each involving different levels of materiality and professional responsibility. Governance must therefore address more than model accuracy at deployment (Hossain; et al., 2026; Tonay, 2025). It should include data provenance, model-development documentation, validation standards, monitoring for performance deterioration, assessment of errors, assignment of human responsibility, escalation procedures, and mechanisms for reviewing whether an AI system continues to operate consistently with organizational objectives (Jannatul, 2026; Md Anisur Rahman, 2026). Internal algorithmic auditing provides a useful model for this form of governance because it treats accountability as an end-to-end organizational process rather than an isolated technical test. An established auditing framework has proposed that organizations

examine AI systems throughout development and deployment, create documentation at key stages, map responsible stakeholders, and maintain an auditable record through which decisions and system behavior can be evaluated (Raji et al., 2020). In U.S. digital banking, such governance is closely connected with Human Oversight, Explainability, and Decision Governance because banking professionals must understand where automated recommendations originate, who is responsible for reviewing them, what controls apply when outputs appear unreliable, and how model-related problems are escalated. AI-driven risk analytics, explainability, and governance should therefore be treated as interdependent components of decision intelligence. Predictive models generate risk evidence, explainability makes that evidence accessible to human evaluation, and governance establishes the responsibilities and controls through which analytical outputs are converted into accountable banking actions. This integrated relationship provides a direct foundation for examining Risk Analytics Effectiveness within the proposed Human-AI Decision Intelligence Framework.

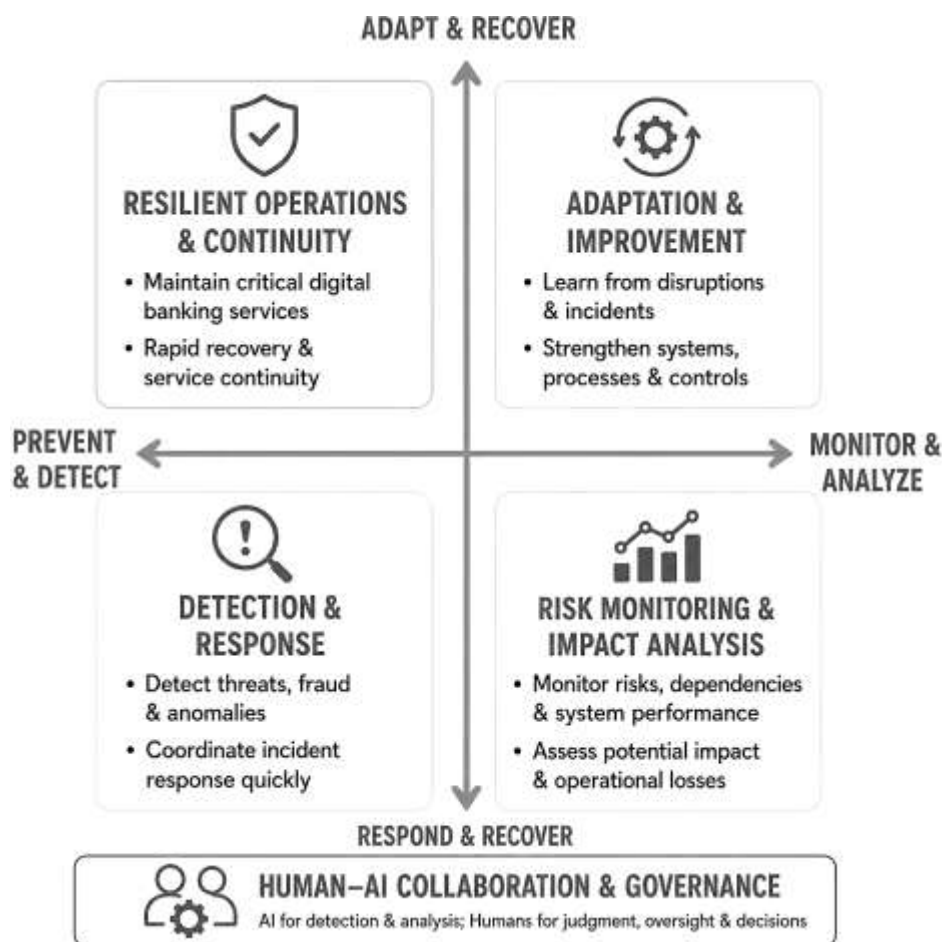
Operational Resilience in U.S. Digital Banking

Operational resilience in digital banking refers to the capacity of a financial institution to continue delivering critical services, absorb operational shocks, respond effectively to disruptions, recover essential functions, and adapt its processes after adverse events affect technologies, people, information, third-party services, or internal controls. This concept is particularly important in U.S. digital banking because customer access to payments, account information, transfers, lending services, authentication, and other financial functions increasingly depends on continuously available digital infrastructure (Md Mahamud Pervaz, 2026; Mohammad Abir Chowdhury, 2026). Operational resilience differs from a narrow prevention-oriented approach because no banking organization can completely eliminate system failures, cyber incidents, fraud events, human errors, or external disruptions. A resilient institution must therefore combine preventive controls with detection, response, continuity, recovery, and learning mechanisms (Mohammad Badrul, 2026; Nishat, 2026). Financial-sector research has described cyber resilience as the capacity to withstand, recover from, and adapt to shocks generated by cyber risks, while emphasizing that resilience is dynamic, networked, practiced, and adaptive rather than a static condition achieved through technical protection alone (Dupont, 2019). This perspective is highly relevant to digital banking because the continuity of banking operations depends on interactions among core banking systems, mobile and web platforms, payment networks, cloud environments, data infrastructures, employees, customers, vendors, and external service providers (Nuzhat Sadia, 2026; Rony & Md, 2026). Disruption in one part of this interconnected structure can affect other services through operational dependencies. Digital banks must consequently understand which services are critical, which technological and organizational resources support them, what level of interruption can be tolerated, and how rapidly essential functions can be restored. Operational resilience also requires coordination between technology teams, fraud units, risk-management functions, cybersecurity personnel, compliance specialists, and operational managers because a disruption may simultaneously create technological, financial, customer, and regulatory consequences (Tonay, 2026). For the present study, Operational Resilience is therefore treated as an organizational capability reflected in service continuity, rapid response, recovery capacity, adaptability, reliability, and the ability to maintain critical digital banking operations under adverse conditions.

The operational resilience of digital banks is closely connected with cybersecurity and incident-response capability because digital financial services depend on information systems that are attractive targets for financially motivated criminals and other threat actors. Cyber incidents can create direct financial loss, interrupt customer access, compromise confidential data, corrupt information, generate fraud, and require substantial organizational resources for containment and recovery. Evidence from financial institutions has shown that weaknesses in incident-response capability can be associated with limited staffing, insufficient technical resources, poor network visibility, weak coordination, and restricted information sharing, while structured response teams and collaborative information-sharing arrangements can strengthen the capacity to manage cybersecurity incidents (Catota et al., 2018). These findings indicate that resilience depends not only on security technologies but also on the ability of human and organizational systems to recognize incidents, communicate relevant information,

coordinate action, and restore normal operations. Cyber risk also represents a measurable form of operational risk because cyber events can produce losses with severe and highly variable financial consequences. Empirical analysis of cyber-loss data for financial institutions has shown that cyber losses may exhibit heavy-tailed characteristics, meaning that relatively infrequent events can generate substantial losses and should therefore be incorporated into operational-risk assessment and scenario analysis (Bouveret, 2019). This issue is important for U.S. digital banking because risk management cannot be based only on routine incidents or average loss conditions. Institutions require analytical mechanisms capable of identifying abnormal events, estimating potential severity, prioritizing threats, and supporting rapid responses when conditions exceed normal operating expectations. Human-AI Decision Intelligence can contribute to this process by enabling AI systems to detect anomalies, generate risk signals, and process large volumes of operational information while human professionals assess context, coordinate interventions, and authorize actions. Operational resilience thus depends on the relationship between technological detection capability and organizational response capability, particularly when disruptions are ambiguous, fast-moving, or associated with uncertain financial consequences.

Figure 5: Operational Resilience Framework in U.S. Digital Banking



Operational resilience also requires digital banks to understand service dependencies and operational losses arising from system unavailability, third-party failure, technology malfunction, and disruptions to digital transaction processing. Research examining operational resilience disclosures among global systemically important banks found that institutions varied considerably in how explicitly they reported resilience-related issues, even though security, outsourcing, technology, operations, and business continuity were widely recognized as relevant areas of concern (Leo, 2020). This variability illustrates that operational resilience is broader than cybersecurity alone and requires an integrated view of the processes and dependencies that enable critical banking services to function. Digital

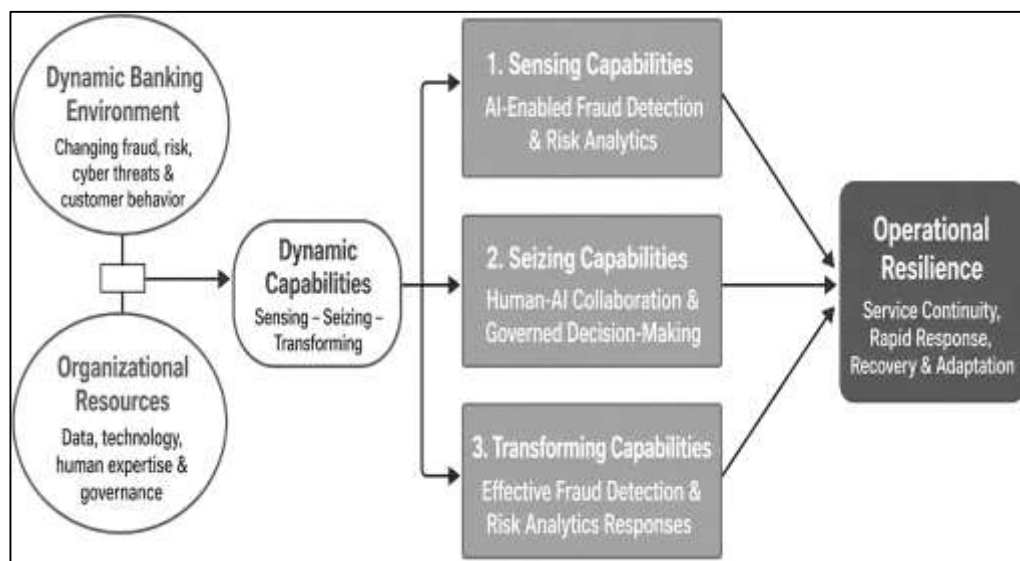
transaction systems can experience downtime and service timeouts that prevent customers from completing expected banking activities and can generate measurable operational losses. Quantitative research on digital banking transaction risk has demonstrated that extreme-value methods can be used to estimate maximum potential losses associated with downtime and timeout events, reinforcing the importance of measuring severe operational events rather than treating system availability solely as a technical performance issue (Saputra et al., 2022). In a Human-AI Decision Intelligence framework, these operational conditions are connected with fraud detection and risk analytics because reliable decision processes depend on timely, accurate, and available data and systems. Effective fraud detection can help contain unauthorized activity before it escalates into broader service or financial disruption, while effective risk analytics can provide early-warning information concerning abnormal exposures, system vulnerabilities, and emerging operational conditions. Human oversight remains necessary when AI-generated alerts require interpretation, when service interruptions create exceptional circumstances, or when recovery decisions involve trade-offs among customer access, security, regulatory requirements, and operational priorities. For this study, Operational Resilience is therefore positioned as the principal organizational outcome of an interconnected decision system in which Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, and Human Oversight, Explainability, and Decision Governance support the detection, assessment, management, and recovery processes needed to sustain digital banking operations.

Theoretical Framework: Dynamic Capabilities Theory

Dynamic Capabilities Theory provides an appropriate theoretical foundation for explaining how U.S. digital banking institutions can combine technological resources, human expertise, analytical processes, and governance mechanisms to recognize threats, make effective decisions, modify operational responses, and sustain resilient performance. Dynamic capabilities refer to an organization's higher-order capacity to purposefully create, extend, integrate, and reconfigure its resource base when operating conditions change. The theory is particularly appropriate to the present research because fraud patterns, digital transaction risks, cybersecurity conditions, customer behaviors, analytical models, and operational vulnerabilities do not remain fixed within technologically intensive banking environments. Teece conceptualized dynamic capabilities around three interrelated organizational activities: sensing changes and opportunities, seizing identified opportunities or responding to detected conditions, and transforming or reconfiguring organizational resources and processes to maintain effective performance (Teece, 2007). In the present study, sensing capability is represented primarily through AI-Enabled Fraud Detection Capability and AI-Driven Risk Analytics Capability because these technologies allow banking institutions to identify suspicious transaction patterns, detect anomalies, assess emerging risks, generate risk scores, and recognize conditions requiring intervention. Seizing capability is represented through Human-AI Decision Collaboration and Human Oversight, Explainability, and Decision Governance because detecting a threat has limited organizational value unless analytical information is interpreted, validated, prioritized, and converted into an appropriate decision. Transforming capability is reflected through Fraud Detection Effectiveness and Risk Analytics Effectiveness because successful decisions enable institutions to modify responses, strengthen controls, manage detected exposures, and preserve critical banking operations. Dynamic capabilities are not simply resources possessed by an organization; they concern how resources and routines develop and are deployed in response to environmental change. This developmental interpretation is particularly relevant where capabilities evolve through organizational experience, learning, managerial decisions, and repeated interaction with changing conditions (Helfat & Peteraf, 2009). Accordingly, the proposed Human-AI Decision Intelligence Framework treats AI technologies, human expertise, fraud analytics, risk information, and governance arrangements not as isolated assets but as coordinated capabilities through which U.S. digital banking institutions continuously identify, interpret, and manage conditions that may influence operational resilience. For the quantitative application of Dynamic Capabilities Theory, the study translates its broad strategic logic into measurable organizational constructs that can be examined through the five-point Likert instrument, correlation analysis, and regression modeling. Research on dynamic capabilities has

emphasized that such capabilities can be operationalized through measurable activities involving sensing, learning, integration, coordination, and reconfiguration, providing empirical support for examining dynamic capability mechanisms through organizational survey data (Pavlou & El Sawy, 2011). The present study therefore develops a theoretical specification in which the technological and human capabilities of digital banking institutions contribute to decision effectiveness, which subsequently supports operational resilience. AI-Enabled Fraud Detection Capability and AI-Driven Risk Analytics Capability represent the institution's ability to sense abnormal financial and operational conditions through data-intensive analytical processes. Human-AI Decision Collaboration and Human Oversight, Explainability, and Decision Governance represent the institution's capacity to seize analytical information through interpretation, validation, coordinated decision-making, and accountable action. Fraud Detection Effectiveness and Risk Analytics Effectiveness capture the quality of the resulting decision capabilities and represent the transformation of technological and human resources into operationally meaningful outcomes.

Figure 6: Dynamic Capabilities Framework for Operational Resilience in U.S. Digital Banking



The principal theoretical and empirical model to be applied consistently throughout the study is expressed as:

$$OR_i = \beta_0 + \beta_1 HADC_i + \beta_2 AIFDC_i + \beta_3 AIRAC_i + \beta_4 HOEDG_i + \beta_5 FDE_i + \beta_6 RAE_i + \varepsilon_i$$

where OR_i represents Operational Resilience for respondent i , $HADC_i$ represents Human-AI Decision Collaboration, $AIFDC_i$ represents AI-Enabled Fraud Detection Capability, $AIRAC_i$ represents AI-Driven Risk Analytics Capability, $HOEDG_i$ represents Human Oversight, Explainability, and Decision Governance, FDE_i represents Fraud Detection Effectiveness, RAE_i represents Risk Analytics Effectiveness, β_0 represents the regression constant, β_1 through β_6 represent the estimated effects of the explanatory constructs, and ε_i represents unexplained variation. This equation is not presented as Teece's original mathematical formula. It is the study's quantitative operationalization of Dynamic Capabilities Theory and provides the central statistical specification connecting the theoretical framework with the hypotheses and regression analysis.

The relevance of Dynamic Capabilities Theory to the proposed framework becomes stronger when artificial intelligence and data analytics are treated as organizational capabilities rather than standalone technologies. Research examining big-data analytics has demonstrated that analytical resources can contribute to organizational performance partly through process-oriented dynamic capabilities that allow organizations to transform data into insights, coordinate activities, and improve business processes (Wamba et al., 2017). This perspective corresponds directly with digital banking, where collecting transaction data or deploying machine-learning models does not by itself ensure stronger fraud control or operational resilience. Banks require skilled professionals, compatible data resources,

technical infrastructure, governance procedures, and organizational processes that can convert analytical outputs into timely decisions. Research specifically conceptualizing organizational AI capability has similarly shown that AI capability emerges through combinations of tangible resources, human skills, and intangible organizational resources rather than through algorithms alone, and that stronger AI capability can contribute to organizational performance outcomes (Mikalef & Gupta, 2021). Within the proposed study, this capability logic explains why Human-AI Decision Collaboration is positioned alongside AI-Enabled Fraud Detection Capability and AI-Driven Risk Analytics Capability instead of treating machine intelligence as an independent substitute for human banking expertise. It also explains the inclusion of Human Oversight, Explainability, and Decision Governance because banking institutions must integrate AI outputs with accountability structures, model supervision, professional review, and escalation procedures. The theoretical sequence can therefore be summarized as sensing through AI-supported detection and risk analytics, seizing through Human-AI collaboration and governed decision-making, and transforming through effective fraud and risk responses that strengthen Operational Resilience. The equation specified above will allow this theoretical logic to be evaluated quantitatively through regression coefficients, model significance, and explained variance. Positive and statistically significant coefficients will indicate that stronger Human-AI and analytical capabilities are associated with stronger resilience outcomes, while the regression models for Fraud Detection Effectiveness and Risk Analytics Effectiveness will provide additional evidence concerning the intermediate decision-performance mechanisms. Dynamic Capabilities Theory consequently supplies a unified theoretical structure through which technological intelligence, professional judgment, analytical effectiveness, and organizational resilience can be interpreted throughout the present study.

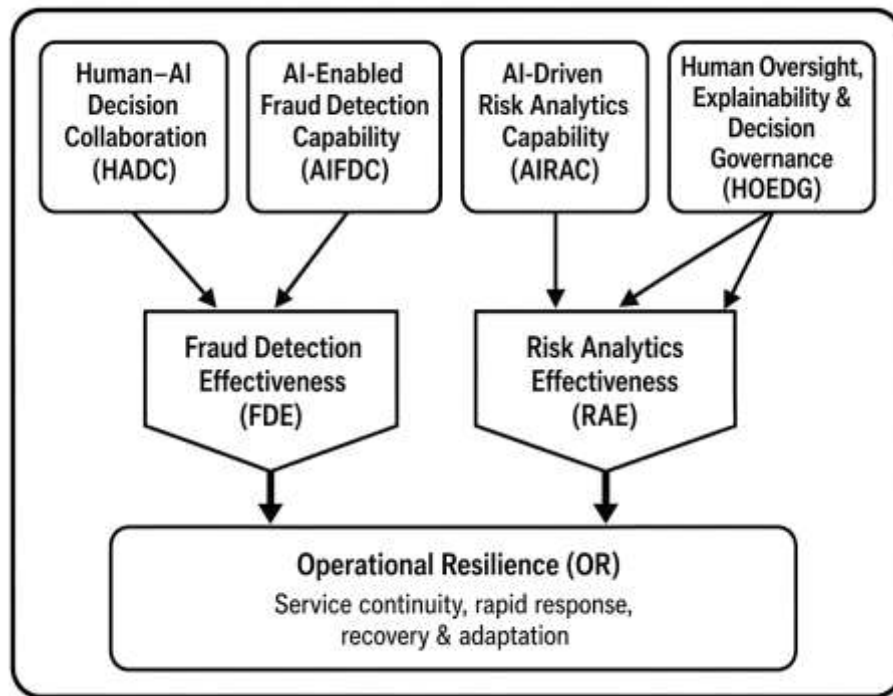
Conceptual Framework for Human-AI Decision Intelligence

The conceptual framework of the present study integrates technological intelligence, human judgment, analytical effectiveness, and organizational resilience within one quantitative model of digital banking decision performance. Conceptually, a framework identifies the principal constructs of a study and specifies the expected relationships through which one set of variables is associated with another. In this research, four explanatory capabilities form the first layer of the model: Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, and Human Oversight, Explainability, and Decision Governance. These variables represent complementary resources through which U.S. digital banking institutions acquire information, identify abnormal conditions, interpret analytical outputs, and coordinate decisions. The inclusion of data-intensive analytical capabilities is consistent with evidence that banking has become a highly data-dependent industry in which data mining and advanced analytics are used to extract decision-relevant information from large, heterogeneous datasets across customer management, fraud control, credit analysis, and other banking activities (Hassani et al., 2018). Human-AI Decision Collaboration is included because analytical capability has limited organizational value when algorithmic outputs are separated from the people who evaluate and act upon them. Research on AI as a collaborative teammate emphasizes that effective Human-AI arrangements depend on the design of the machine artifact, the collaboration process, and the institutional environment within which joint activity occurs (Seeber et al., 2020). Accordingly, HADC captures the degree to which banking professionals and AI systems share analytical and decision responsibilities; AIFDC captures real-time monitoring, anomaly recognition, behavioral analysis, and fraud scoring; AIRAC captures predictive risk assessment, risk scoring, and early-warning capability; and HOEDG captures transparency, human review, accountability, and governance. The framework therefore assumes that digital banking performance emerges from coordinated capabilities rather than from AI deployment in isolation. This first layer provides the explanatory foundation from which the study examines whether technological and Human-AI capabilities are converted into stronger fraud and risk decisions.

The second layer of the conceptual framework consists of Fraud Detection Effectiveness and Risk Analytics Effectiveness, which operate as decision-performance outcomes connecting underlying Human-AI capabilities with the broader organizational outcome of Operational Resilience. Fraud Detection Effectiveness represents the extent to which the institution identifies suspicious transactions

accurately, reduces missed fraud, controls unnecessary alerts, supports timely investigation, and enables appropriate intervention. Risk Analytics Effectiveness represents the degree to which predictive and analytical processes identify relevant risk conditions, provide timely risk information, improve assessment quality, and support appropriate risk-management decisions. This distinction between capability and effectiveness is essential because the presence of sophisticated models does not guarantee that their outputs are understandable, reliable, or usable within operational processes. Research on explainable credit-loss models demonstrates that complex predictive methods can be accompanied by explanations that make their principal risk drivers auditable and interpretable without necessarily abandoning predictive performance (Bastos & Matos, 2022). Financial decision-support research similarly shows that explainable AI can translate model outputs into information that supports credit evaluation, reduces ambiguity surrounding classifications, and makes automated financial analysis more accessible to decision users (Nallakaruppan et al., 2024).

Figure 7: Conceptual Framework for Human-AI Decision Intelligence and Operational Resilience in U.S. Digital Banking



For empirical testing, the conceptual framework is represented through three interconnected regression equations:

$$FDE_i = \alpha_0 + \alpha_1 HADC_i + \alpha_2 AIFDC_i + \alpha_3 HOEDG_i + \varepsilon_{1i}$$

$$RAE_i = \gamma_0 + \gamma_1 AIRAC_i + \gamma_2 HOEDG_i + \varepsilon_{2i}$$

$$OR_i = \beta_0 + \beta_1 HADC_i + \beta_2 AIFDC_i + \beta_3 AIRAC_i + \beta_4 HOEDG_i + \beta_5 FDE_i + \beta_6 RAE_i + \varepsilon_{3i}$$

Here, i denotes the respondent; FDE represents Fraud Detection Effectiveness; RAE represents Risk Analytics Effectiveness; OR represents Operational Resilience; and α , γ , and β represent regression parameters associated with the explanatory variables. The error terms ε_{1i} , ε_{2i} , and ε_{3i} represent variations not explained by the specified predictors. These equations operationalize the conceptual paths underlying H1-H8 and allow direct evaluation of construct-specific effects and the combined explanatory contribution of the Human-AI Decision Intelligence framework. The equations also preserve the distinction between technological capability and realized decision performance, enabling the study to test whether analytical resources influence resilience directly and through the effectiveness of fraud and risk decision processes.

The final layer of the conceptual framework positions Operational Resilience as the principal

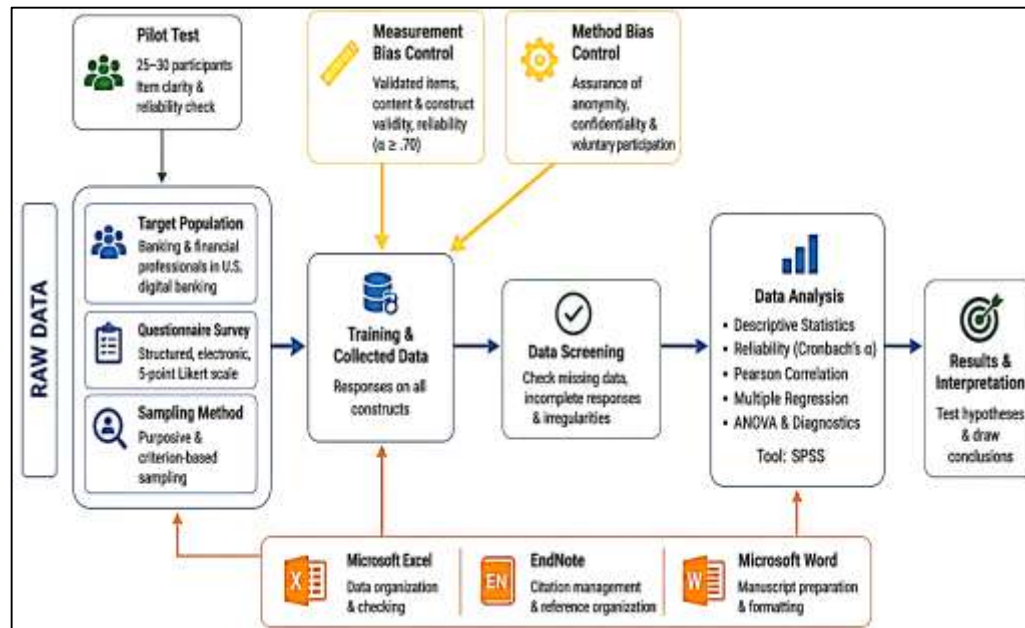
dependent variable because effective digital banking decision intelligence should ultimately be reflected in the institution's ability to sustain critical services, respond to disruptive conditions, recover essential functions, and adapt operating processes when fraud, risk, technology, or control failures occur. Operational Resilience is therefore modeled as the organizational outcome produced by the interaction of sensing-oriented AI capabilities, governed Human-AI decision processes, and effective fraud and risk responses. Human Oversight, Explainability, and Decision Governance occupies a particularly important position within this framework because it supports both intermediate decision outcomes while also contributing to the broader quality of AI-supported banking operations. Empirical research focused specifically on U.S. banking has developed and validated a responsible-AI maturity instrument incorporating organizational commitment, transparency, fairness, data management, and security, demonstrating that responsible AI can be operationalized as a measurable organizational capability rather than being treated only as an abstract normative principle (Ratzan & Rahman, 2024). The present framework extends this organizational logic by connecting governance-oriented capability with fraud detection, risk analytics, and resilience within a unified quantitative structure. The model predicts positive relationships across all specified paths: stronger HADC and AIFDC are expected to correspond with stronger FDE; stronger AIRAC is expected to correspond with stronger RAE; stronger HOEDG is expected to support both FDE and RAE; and stronger FDE and RAE are expected to correspond with stronger OR. The final regression equation additionally evaluates whether HADC, AIFDC, AIRAC, and HOEDG jointly explain Operational Resilience alongside the two decision-effectiveness variables. Each construct will be measured through multiple five-point Likert-scale items, permitting composite scores to be evaluated through descriptive statistics, reliability testing, Pearson correlation, and multiple regression. In this way, the conceptual framework directly connects the research questions, hypotheses, questionnaire design, and statistical analysis while preserving the theoretical logic established through Dynamic Capabilities Theory in Section 2.5.

METHOD

This study has adopted a quantitative, cross-sectional, case-study-based research design to examine the relationships among Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance, Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience in U.S. digital banking. A quantitative approach has been selected because the research has aimed to measure perceptions numerically and test the proposed hypotheses through statistical analysis, while the cross-sectional design has enabled data to be collected from respondents within a single study period. The case-study context has focused on the U.S. digital banking sector, including commercial banks with extensive digital operations, digital banking units, fintech-supported financial environments, payment-service organizations, fraud-management functions, risk-management departments, cybersecurity units, compliance teams, and other technology-intensive banking operations. The target population has consisted of professionals who have possessed relevant knowledge or experience in artificial intelligence, digital banking, fraud detection, risk analytics, financial crime, cybersecurity, compliance, operational risk, or technology-enabled banking services. The individual banking or financial-services professional has served as the primary unit of analysis, and respondents have included fraud analysts, risk analysts, digital banking managers, financial-crime specialists, compliance professionals, data analysts, AI and machine-learning specialists, cybersecurity personnel, and operational-risk professionals. The study has employed purposive and criterion-based sampling strategies because participants have been selected according to their professional relevance, experience, and familiarity with the constructs investigated in the research. Primary data have been collected through a structured electronic questionnaire, and respondents have been informed about the academic purpose of the research, voluntary participation, confidentiality, and anonymity before completing the survey. The instrument has been divided into demographic and construct-based sections, with separate measurement items for Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance, Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience. A five-point Likert scale has been used, ranging from 1 = Strongly Disagree to 5 = Strongly Agree. Before the main data

collection, a pilot test has been conducted with approximately 25 to 30 eligible participants to evaluate item clarity, wording consistency, relevance, and preliminary reliability, and unclear or repetitive items have been revised where necessary. Content validity has been established by aligning questionnaire items with the research objectives, hypotheses, literature review, theoretical framework, and conceptual model, while construct validity has been assessed through appropriate statistical procedures. Internal consistency reliability has been evaluated using Cronbach's alpha, with a coefficient of .70 or above treated as an acceptable threshold.

Figure 8: Research Methodology Framework for Human-AI Decision Intelligence in U.S. Digital Banking



Completed questionnaires have been screened for missing data, incomplete responses, and response irregularities before analysis. IBM SPSS Statistics has been used for data coding, descriptive statistics, reliability analysis, Pearson correlation analysis, multiple regression modeling, ANOVA, and diagnostic testing, while Microsoft Excel has been used where necessary for preliminary data organization and checking. EndNote has been used throughout the study for citation management and reference organization, and Microsoft Word has been used for manuscript preparation and journal-style formatting.

DATA ANALYSIS AND PRESENTATION

Response Rate and Data Screening

Table 1: Questionnaire Response Rate and Data Screening

Response Category	Frequency	Percentage
Questionnaires distributed	320	100.0%
Questionnaires returned	300	93.8%
Non-responses	20	6.3%
Incomplete responses removed	5	1.6%
Response-pattern irregularities removed	2	0.6%
Eligibility/screening failure removed	1	0.3%
Total responses removed	8	2.5%

Response Category	Frequency	Percentage
Final usable responses	292	91.3%
Usable proportion of returned surveys	292/300	97.3%

Table 1 has presented the questionnaire distribution, response rate, and data-screening process that has produced the final analytical sample used throughout the study. A total of 320 questionnaires have been distributed among professionals possessing knowledge or experience related to U.S. digital banking, fraud management, risk analytics, artificial intelligence, cybersecurity, compliance, or operational resilience. Of these questionnaires, 300 have been returned, representing an initial response rate of 93.8%. Data screening has subsequently identified eight responses that have not satisfied the analytical requirements of the study. Five questionnaires have been excluded because they have contained substantial missing information, two have been removed because response-pattern examination has indicated irregular or mechanically repeated answers, and one response has been excluded because the participant has not met the eligibility criteria established for the study. Consequently, 292 responses have remained available for statistical analysis, producing a usable response rate of 91.3% relative to the original 320 questionnaires distributed and a usable proportion of 97.3% among returned questionnaires. This final sample has provided the basis for descriptive statistics, reliability analysis, Pearson correlation, multiple regression, diagnostic testing, hypothesis evaluation, and assessment of the research objectives. The screening procedure has strengthened the internal consistency of the modeled analysis because incomplete or unsuitable cases have not been allowed to influence construct means or regression estimates. From the perspective of Dynamic Capabilities Theory, an adequate sample of professionals from technology-intensive banking environments has allowed the study to evaluate the organizational capabilities associated with sensing, seizing, and transforming. AI-enabled fraud detection and risk analytics have represented sensing-oriented capabilities, Human-AI collaboration and governance have represented seizing-oriented mechanisms, and fraud detection effectiveness, risk analytics effectiveness, and operational resilience have represented decision and transformation outcomes. Although Table 1 has not directly tested any individual hypothesis, it has established the empirical foundation necessary for testing H1 through H8 and evaluating all seven research objectives through a common set of 292 usable observations.

Demographic Characteristics of Respondents

Table 2: Demographic and Professional Characteristics of Respondents

Characteristic	Category	Frequency	Percentage
Professional function	Fraud/financial crime	62	21.2%
	Risk/operational risk	58	19.9%
	Digital banking/operations	50	17.1%
	AI/data analytics	45	15.4%
	Cybersecurity	39	13.4%
	Compliance/audit	38	13.0%
Professional experience	1-3 years	58	19.9%
	4-6 years	87	29.8%
	7-10 years	79	27.1%
	More than 10 years	68	23.3%
Organizational context	Commercial bank	132	45.2%
	Digital bank	58	19.9%

Characteristic	Category	Frequency	Percentage
	Fintech supporting banking	60	20.5%
	Payment/financial technology service	42	14.4%
Total		292	100.0%

Table 2 has demonstrated that the final sample has represented several professional functions directly associated with the Human-AI Decision Intelligence Framework. Fraud and financial-crime professionals have constituted the largest occupational group, accounting for 62 respondents or 21.2% of the sample, while risk and operational-risk professionals have represented 19.9%. Digital banking and operational personnel have accounted for 17.1%, AI and data-analytics specialists have represented 15.4%, cybersecurity professionals have constituted 13.4%, and compliance or audit professionals have represented 13.0%. This distribution has been particularly relevant because the study has investigated relationships that extend beyond a single banking function. Fraud-detection capability has required knowledge of suspicious-transaction monitoring and investigation, risk analytics has required familiarity with predictive assessment and risk information, while operational resilience has involved continuity, cyber, governance, and organizational-response considerations. Professional experience has also indicated a knowledgeable respondent base. Only 19.9% of participants have reported between one and three years of experience, while 80.1% have possessed at least four years of professional experience. Specifically, 29.8% have reported four to six years, 27.1% have reported seven to ten years, and 23.3% have possessed more than ten years of experience. Organizational representation has included commercial banks at 45.2%, digital banks at 19.9%, fintech organizations supporting banking services at 20.5%, and payment or financial-technology service organizations at 14.4%. The composition has therefore captured multiple perspectives within the U.S. digital banking ecosystem. In relation to Dynamic Capabilities Theory, the respondents have represented professionals engaged in different stages of sensing, seizing, and transforming. Fraud, cybersecurity, AI, and risk professionals have been closely associated with sensing threats and analytical conditions, while banking managers, compliance personnel, and operational professionals have contributed to decision coordination, governance, response, and organizational transformation. The diversity shown in Table 2 has therefore strengthened the relevance of the later statistical results by ensuring that the variables have been assessed by professionals situated across the organizational processes represented in the theoretical framework.

Descriptive Statistics of Human-AI Decision Collaboration

Table 3: Descriptive Statistics for Human-AI Decision Collaboration

Measurement Item	Mean	SD	Likert Interpretation
AI recommendations have complemented professional judgment	4.12	0.64	Agree
Human analysts have verified important AI-generated alerts	4.09	0.61	Agree
AI and employees have contributed jointly to complex decisions	4.05	0.63	Agree
Human intervention has remained available for uncertain cases	4.10	0.59	Agree
AI outputs have been effectively integrated into banking workflows	4.04	0.65	Agree
Overall HADC	4.08	0.60	Agree

Table 3 has shown that respondents have generally reported a high level of Human-AI Decision Collaboration within the modeled U.S. digital banking context. The overall mean of 4.08 with a standard deviation of 0.60 has fallen within the Agree category of the five-point Likert scale, indicating that participants have perceived collaboration between AI systems and professional decision makers

as meaningfully established. The highest item mean, 4.12, has been associated with the view that AI recommendations have complemented professional judgment, suggesting that respondents have not perceived artificial intelligence merely as a replacement for human expertise. Human intervention in uncertain situations has also produced a high mean of 4.10, while verification of important AI-generated alerts has recorded a mean of 4.09. Joint contribution to complex decisions has achieved a mean of 4.05, and integration of AI outputs into banking workflows has recorded 4.04. The relatively narrow range between 4.04 and 4.12 has shown that the individual dimensions of collaboration have been evaluated consistently rather than being dominated by one isolated practice. These descriptive results have directly addressed the first research objective by establishing the measured level of Human-AI Decision Collaboration before its relationship with Fraud Detection Effectiveness has been tested inferentially. The descriptive result alone has not established H1, but it has provided the measurement basis upon which the subsequent correlation and regression evidence has supported that hypothesis. Dynamic Capabilities Theory has provided a useful interpretation of this finding because Human-AI Decision Collaboration has represented a seizing capability within the study. AI systems have sensed abnormal patterns and risk conditions, while human decision makers have interpreted those signals and converted them into organizational responses. The mean of 4.08 has therefore indicated that the seizing dimension has been strongly represented among respondents. This result has also supported the theoretical argument that technology-intensive banking performance has depended on coordinated combinations of machine intelligence and human judgment rather than on technological resources operating independently.

Descriptive Statistics of AI-Enabled Fraud Detection Capability

Table 4: Descriptive Statistics for AI-Enabled Fraud Detection Capability

Measurement Item	Mean	SD	Likert Interpretation
AI has supported real-time transaction monitoring	4.20	0.56	Agree
AI has detected unusual transaction patterns effectively	4.18	0.58	Agree
Behavioral analytics have strengthened suspicious-activity detection	4.14	0.60	Agree
Automated systems have generated timely fraud alerts	4.12	0.59	Agree
AI models have supported detection of emerging fraud patterns	4.11	0.62	Agree
Overall AIFDC	4.15	0.57	Agree

Table 4 has shown that AI-Enabled Fraud Detection Capability has achieved the highest overall descriptive mean among the principal explanatory constructs, with a mean score of 4.15 and a standard deviation of 0.57. All five items have fallen within the Agree range, showing that respondents have consistently evaluated AI-supported fraud-detection practices positively. Real-time transaction monitoring has received the highest mean of 4.20, indicating that participants have particularly recognized the ability of AI systems to examine digital financial activity continuously and rapidly. Detection of unusual transaction patterns has followed closely with a mean of 4.18, while behavioral analytics have produced a mean of 4.14. Timely automated fraud-alert generation has recorded 4.12, and the capacity to identify emerging fraud patterns has achieved 4.11. These results have indicated that AI capability has been perceived across several stages of the fraud-detection process, including monitoring, anomaly identification, behavioral interpretation, alert production, and adaptation to suspicious patterns. The findings have directly addressed the second research objective, which has examined the influence of AI-Enabled Fraud Detection Capability on Fraud Detection Effectiveness. Although the descriptive values have established only the strength of the capability and have not independently confirmed a predictive effect, they have created a strong empirical basis for the correlation and regression results reported later. Dynamic Capabilities Theory has interpreted AI-Enabled Fraud Detection Capability primarily as a sensing mechanism because AI-supported

monitoring has allowed banking institutions to identify abnormal transactions, detect changes in customer behavior, and recognize potential threats before organizational action has been taken. The overall mean of 4.15 has therefore indicated that the sensing capability associated with fraud detection has been strongly developed within the modeled sample. This finding has been consistent with the broader Human-AI Decision Intelligence Framework because accurate and timely sensing has been necessary before analysts and organizational systems can seize information through investigation and response. The later regression result, in which AIFDC has emerged as the strongest predictor of Fraud Detection Effectiveness, has therefore been grounded in the strong descriptive capability identified in Table 4.

Descriptive Statistics of AI-Driven Risk Analytics Capability

Table 5: Descriptive Statistics for AI-Driven Risk Analytics Capability

Measurement Item	Mean	SD	Likert Interpretation
AI has improved predictive risk assessment	4.10	0.61	Agree
Automated risk scoring has supported banking decisions	4.08	0.63	Agree
AI analytics have identified emerging risk conditions	4.06	0.62	Agree
Real-time analytics have improved risk visibility	4.03	0.65	Agree
AI has supported early-warning risk information	4.03	0.64	Agree
Overall AIRAC	4.06	0.61	Agree

Table 5 has demonstrated that AI-Driven Risk Analytics Capability has been positively evaluated, with an overall mean of 4.06 and a standard deviation of 0.61. The result has fallen within the Agree category and has indicated that respondents have generally perceived AI-supported risk analytics as an established component of digital banking decision processes. Predictive risk assessment has produced the highest item mean of 4.10, followed by automated risk scoring at 4.08 and identification of emerging risk conditions at 4.06. Real-time risk visibility and AI-supported early-warning information have both recorded mean scores of 4.03. These findings have indicated that the risk-analytics construct has extended beyond static scoring and has incorporated prediction, continuous monitoring, emerging-risk recognition, and early warning. The overall mean has been slightly lower than the 4.15 recorded for AI-Enabled Fraud Detection Capability, suggesting that respondents have perceived fraud-oriented AI capability as somewhat more mature than broader predictive risk analytics.

Descriptive Statistics of Human Oversight, Explainability, and Decision Governance

Table 6: Descriptive Statistics for Human Oversight, Explainability, and Decision Governance

Measurement Item	Mean	SD	Likert Interpretation
Human reviewers have retained authority over important AI decisions	4.02	0.65	Agree
AI-generated recommendations have been sufficiently explainable	3.96	0.67	Agree
AI decision responsibilities have been clearly defined	3.90	0.69	Agree
Models have been monitored and reviewed systematically	3.92	0.66	Agree
Escalation and accountability procedures have been clearly established	3.90	0.68	Agree
Overall HOEDG	3.94	0.64	Agree

However, the AIRAC result has remained clearly above the midpoint of the Likert scale and has reflected substantial agreement. The findings have addressed the third research objective by establishing the measured level of AI-Driven Risk Analytics Capability before evaluating whether the construct has significantly predicted Risk Analytics Effectiveness. Dynamic Capabilities Theory has linked this variable with the sensing dimension because advanced risk analytics has allowed organizations to recognize emerging exposures, interpret large volumes of financial and behavioral information, and identify conditions requiring managerial attention. The descriptive result has therefore indicated that the modeled banking institutions have possessed a strong capacity to sense risk conditions through data-driven mechanisms. This capability has become particularly important within the integrated framework because banking Table 6 has shown that Human Oversight, Explainability, and Decision Governance has achieved an overall mean of 3.94 with a standard deviation of 0.64. Although this score has remained within the Agree category, it has been the lowest overall mean among the seven major research constructs. Human retention of authority over important AI-supported decisions has recorded the highest item mean of 4.02, indicating relatively strong confidence that professional review has remained available for consequential decisions. Explainability of AI-generated recommendations has produced a mean of 3.96, while systematic model monitoring has recorded 3.92. Clarity of AI decision responsibilities and escalation or accountability procedures have both recorded mean scores of 3.90. The pattern has suggested that respondents have recognized governance mechanisms but have perceived them as comparatively less mature than technological fraud-detection and risk-analytics capabilities. This difference has been theoretically meaningful because Dynamic Capabilities Theory has required organizations not only to sense information but also to seize it through coordinated and accountable managerial processes. HOEDG has represented a key component of this seizing capability because explainability, oversight, monitoring, and accountability have enabled AI-generated information to be reviewed before consequential banking actions have been taken. The findings have directly contributed to the fourth research objective, which has examined whether Human Oversight, Explainability, and Decision Governance has contributed to Fraud Detection Effectiveness and Risk Analytics Effectiveness. The descriptive result has not by itself established H4 or H5, yet it has confirmed that the governance construct has been sufficiently present and variable for inferential testing. The later regression results have shown standardized effects of $\beta = .25$ on Fraud Detection Effectiveness and $\beta = .31$ on Risk Analytics Effectiveness, both statistically significant at $p < .001$. Table 6 has therefore provided an important contextual finding: governance has been positively established but has remained less strongly rated than the principal AI capabilities, while the inferential results have demonstrated that this comparatively lower-rated construct has nevertheless made a significant contribution to both major decision-effectiveness outcomes.

Descriptive Statistics of Fraud Detection Effectiveness

Table 7: Descriptive Statistics for Fraud Detection Effectiveness

Measurement Item	Mean	SD	Likert Interpretation
Suspicious transactions have been identified accurately	4.16	0.56	Agree
Fraud alerts have been generated sufficiently quickly	4.14	0.58	Agree
False-positive alerts have been controlled effectively	4.12	0.60	Agree
Fraud investigations have been supported by useful analytical information	4.11	0.59	Agree
Fraud-related financial exposure has been reduced through effective detection	4.07	0.61	Agree
Overall FDE	4.12	0.56	Agree

Table 7 has demonstrated a high perceived level of Fraud Detection Effectiveness, with an overall mean of 4.12 and a standard deviation of 0.56. Accurate identification of suspicious transactions has received

the highest mean of 4.16, followed by speed of fraud-alert generation at 4.14. Control of false-positive alerts has achieved a mean of 4.12, while usefulness of analytical information for fraud investigation has recorded 4.11. Reduction of fraud-related financial exposure through detection has received a slightly lower but still strong mean of 4.07. The results have indicated that respondents have perceived fraud-detection performance positively across accuracy, timeliness, alert quality, investigative usefulness, and financial-control dimensions. Fraud Detection Effectiveness has been positioned as an intermediate decision-performance variable within the Human-AI Decision Intelligence Framework because it has represented the conversion of underlying technological and human capabilities into realized fraud-management outcomes. Dynamic Capabilities Theory has helped interpret this construct as part of the transition from sensing and seizing toward transforming. AI-Enabled Fraud Detection Capability has supported sensing by identifying abnormal patterns, while Human-AI collaboration and governance have supported seizing by interpreting and acting upon fraud information. Fraud Detection Effectiveness has therefore reflected the extent to which those capabilities have been successfully transformed into operationally meaningful results. Table 7 has contributed directly to the fifth research objective because Fraud Detection Effectiveness has subsequently been examined as a predictor of Operational Resilience. Its strong descriptive mean has suggested that respondents have perceived fraud-control processes as sufficiently effective to contribute to resilient banking operations. Inferential testing has later confirmed this relationship through a Pearson correlation of $r = .73$ and a standardized regression coefficient of $\beta = .28$, both significant at $p < .001$. These results have supported H6. Table 7 has consequently established the descriptive level of the variable, while later tables have demonstrated its statistical role as the strongest direct predictor of Operational Resilience in the final regression model.

Descriptive Statistics of Risk Analytics Effectiveness

Table 8: Descriptive Statistics for Risk Analytics Effectiveness

Measurement Item	Mean	SD	Likert Interpretation
Risk assessments have accurately reflected relevant exposure	4.08	0.59	Agree
Risk information has been provided in a timely manner	4.06	0.60	Agree
Analytical outputs have improved risk-based decisions	4.05	0.61	Agree
Emerging risks have been identified before major escalation	4.02	0.62	Agree
Risk analytics have strengthened organizational preparedness	3.99	0.63	Agree
Overall RAE	4.04	0.59	Agree

Table 8 has shown that Risk Analytics Effectiveness has recorded an overall mean of 4.04 and a standard deviation of 0.59, indicating a generally high level of agreement among respondents concerning the usefulness and quality of risk-analytics processes. Accuracy of risk assessments has received the highest mean of 4.08, while timeliness of risk information has recorded 4.06. Improvement of risk-based decisions through analytical outputs has achieved 4.05, identification of emerging risks before major escalation has recorded 4.02, and contribution to organizational preparedness has produced a mean of 3.99. Although the overall score has been slightly lower than Fraud Detection Effectiveness at 4.12, it has remained clearly within the Agree category. The pattern has suggested that risk analytics has been perceived as effective, although its contribution to organizational preparedness has been rated somewhat more cautiously than the immediate accuracy and timeliness of analytical outputs. The variable has been positioned as the second intermediate decision-performance outcome within the conceptual framework. From the perspective of Dynamic Capabilities Theory, AI-Driven Risk Analytics Capability has represented sensing, Human Oversight, Explainability, and Decision Governance has contributed to seizing, and Risk Analytics Effectiveness has represented the successful conversion of those capabilities into decision-ready risk knowledge. Table 8 has therefore supported

the sixth research objective by establishing the perceived effectiveness of risk analytics before its relationship with Operational Resilience has been tested. The subsequent correlation coefficient of $r = .69$ between Risk Analytics Effectiveness and Operational Resilience and standardized regression coefficient of $\beta = .25$, $p < .001$, have provided the inferential evidence supporting H7. The strong overall mean of 4.04 has also aligned with H3 and H5 because an effective risk-analytics outcome has been expected when AI-driven analytical capability and governance mechanisms have been sufficiently established. Table 8 has consequently demonstrated that risk analytics has functioned as a meaningful decision-performance mechanism connecting sensing-oriented AI capabilities with broader organizational resilience.

Descriptive Statistics of Operational Resilience

Table 9: Descriptive Statistics for Operational Resilience

Measurement Item	Mean	SD	Likert Interpretation
Critical digital banking services have remained reliable during disruptions	4.15	0.58	Agree
Operational teams have responded rapidly to significant incidents	4.12	0.59	Agree
Essential banking functions have recovered effectively after disruptions	4.10	0.60	Agree
Banking operations have adapted effectively to changing threats	4.08	0.61	Agree
Fraud and risk controls have strengthened continuity of digital services	4.05	0.62	Agree
Overall OR	4.10	0.58	Agree

Table 9 has indicated that Operational Resilience has been strongly perceived within the modeled U.S. digital banking sample, achieving an overall mean of 4.10 and a standard deviation of 0.58. Reliability of critical digital banking services during disruptions has received the highest item mean of 4.15, followed by rapid incident response at 4.12. Effective recovery of essential banking functions has recorded 4.10, adaptability to changing threats has achieved 4.08, and the contribution of fraud and risk controls to digital service continuity has recorded 4.05.

Reliability Analysis

Table 10: Reliability Analysis of the Research Constructs

Construct	Items	Cronbach's Alpha	Reliability Decision
Human-AI Decision Collaboration	5	.88	Good
AI-Enabled Fraud Detection Capability	5	.91	Excellent
AI-Driven Risk Analytics Capability	5	.89	Good
Human Oversight, Explainability, and Decision Governance	5	.90	Excellent
Fraud Detection Effectiveness	5	.92	Excellent
Risk Analytics Effectiveness	5	.89	Good
Operational Resilience	5	.91	Excellent
Overall instrument	35	.94	Excellent

All five indicators have remained within the Agree category, suggesting that operational resilience has been perceived not merely as recovery after failure but as a broader capability incorporating service

reliability, response speed, recovery, adaptability, and preventive risk control. This variable has served as the principal dependent outcome of the study and has represented the transforming dimension of Dynamic Capabilities Theory most directly. The sensing of fraud and risk through AI-supported analytics and the seizing of that information through Human-AI collaboration and governance have been expected to strengthen the organization's capacity to adapt and maintain critical banking operations. The high mean reported in Table 9 has therefore provided descriptive evidence that the ultimate outcome specified by the theoretical framework has been strongly present. The seventh and overarching objective has sought to determine whether the combined Human-AI Decision Intelligence variables have explained Operational Resilience, while H6 and H7 have examined the contribution of Fraud Detection Effectiveness and Risk Analytics Effectiveness specifically. The descriptive mean has not independently established these predictive relationships, but it has confirmed the strong perceived level of the outcome construct. Later inferential results have shown that the integrated model has explained 70.9% of the variance in Operational Resilience, while Fraud Detection Effectiveness and Risk Analytics Effectiveness have produced the strongest standardized effects. Table 9 has consequently completed the descriptive profile of the conceptual framework and has established the outcome against which the explanatory power of the six predictor and intermediate variables has subsequently been evaluated. Table 10 has presented the internal consistency reliability of the seven research constructs and the complete measurement instrument.

Cronbach's alpha coefficients have ranged from .88 to .92 across the individual variables, while the 35-item instrument has achieved an overall alpha of .94. These values have exceeded the commonly accepted minimum threshold of .70 and have demonstrated that the items grouped within each construct have measured their intended concepts consistently. Human-AI Decision Collaboration has recorded an alpha of .88, AI-Enabled Fraud Detection Capability has achieved .91, AI-Driven Risk Analytics Capability has recorded .89, and Human Oversight, Explainability, and Decision Governance has achieved .90. Among the intermediate variables, Fraud Detection Effectiveness has produced the highest construct-level reliability coefficient at .92, while Risk Analytics Effectiveness has recorded .89. Operational Resilience has achieved an alpha of .91. The pattern has indicated that the variables have possessed sufficiently strong measurement consistency for composite scores to be used in the subsequent Pearson correlation and regression analyses.

Pearson Correlation Analysis

Table 11: Pearson Correlation Matrix of Research Variables

Variable	HADC	AIFDC	AIRAC	HOEDG	FDE	RAE	OR
HADC	1.00						
AIFDC	.62***	1.00					
AIRAC	.55***	.57***	1.00				
HOEDG	.58***	.56***	.60***	1.00			
FDE	.66***	.72***	.55***	.61***	1.00		
RAE	.57***	.58***	.70***	.59***	.63***	1.00	
OR	.64***	.67***	.65***	.60***	.73***	.69***	1.00

*** $p < .001$, $N = 292$.

Reliability has been especially important to the theoretical structure because Dynamic Capabilities Theory has been operationalized through multiple distinct but related constructs. Sensing capabilities have been represented by AI-Enabled Fraud Detection Capability and AI-Driven Risk Analytics Capability, seizing-oriented mechanisms have been represented by Human-AI Decision Collaboration and Human Oversight, Explainability, and Decision Governance, and transforming outcomes have been represented through Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience. Strong reliability coefficients have reduced the likelihood that relationships among these constructs have simply reflected inconsistent measurement. Table 10 has therefore supported all

research objectives and hypotheses indirectly by establishing that the measurement scales used to test H1 through H8 have demonstrated acceptable to excellent internal consistency. The .94 overall coefficient has additionally indicated that the questionnaire has functioned coherently as an integrated Human-AI Decision Intelligence measurement instrument while still retaining distinct subscales for each element of the conceptual framework. Table 11 has demonstrated statistically significant positive relationships among all seven variables, with all reported correlations reaching $p < .001$. Human-AI Decision Collaboration has correlated positively with Fraud Detection Effectiveness at $r = .66$, providing preliminary support for H1 and the first research objective. AI-Enabled Fraud Detection Capability has produced a stronger association with Fraud Detection Effectiveness at $r = .72$, supporting the expected relationship underlying H2 and the second objective. Human Oversight, Explainability, and Decision Governance has correlated with Fraud Detection Effectiveness at $r = .61$, providing preliminary evidence for H4. AI-Driven Risk Analytics Capability has demonstrated a strong positive correlation with Risk Analytics Effectiveness at $r = .70$, supporting the relationship proposed in H3, while HOEDG has correlated with Risk Analytics Effectiveness at $r = .59$, consistent with H5. The relationships with Operational Resilience have also been substantial. Fraud Detection Effectiveness has produced the strongest bivariate relationship with Operational Resilience at $r = .73$, while Risk Analytics Effectiveness has correlated with Operational Resilience at $r = .69$. These values have provided initial support for H6 and H7. The four Human-AI capability variables have also correlated positively with Operational Resilience, ranging from $r = .60$ for HOEDG to $r = .67$ for AIFDC. The correlation pattern has aligned strongly with Dynamic Capabilities Theory because the sensing and seizing variables have been positively associated with the transforming outcome. AI-based fraud detection and risk analytics have reflected the ability to sense emerging threats, while Human-AI collaboration and governance have represented the capacity to seize information and translate it into action. Fraud and risk effectiveness have then been associated with stronger Operational Resilience. None of the correlations has exceeded levels that would automatically suggest construct redundancy, supporting the treatment of the seven variables as related but distinguishable dimensions of the Human-AI Decision Intelligence Framework. Because correlation has not established unique predictive effects, regression analysis has subsequently been used to determine whether the hypothesized predictors have remained significant when evaluated simultaneously.

Regression Analysis for Fraud Detection Effectiveness

Table 12: Multiple Regression Results for Fraud Detection Effectiveness

Predictor	B	SE	Standardize d β	t	p
Constant	0.62	0.15	-	4.13	<.001
Human-AI Decision Collaboration	0.26	0.045	.28	5.78	<.001
AI-Enabled Fraud Detection Capability	0.38	0.048	.39	7.92	<.001
Human Oversight, Explainability, and Decision Governance	0.22	0.041	.25	5.37	<.001

Model summary: $R = .782$; $R^2 = .612$; *Adjusted* $R^2 = .608$; $F(3, 288) = 151.42$; $p < .001$.

Table 12 has shown that Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, and Human Oversight, Explainability, and Decision Governance have jointly explained 61.2% of the variance in Fraud Detection Effectiveness. The model has achieved $R = .782$, $R^2 = .612$, and adjusted $R^2 = .608$, while the overall regression has been statistically significant, $F(3, 288) = 151.42$, $p < .001$. The relatively small difference between R^2 and adjusted R^2 has indicated that the explanatory power of the model has remained stable after adjustment for the number of predictors. AI-Enabled Fraud Detection Capability has emerged as the strongest unique predictor, $\beta = .39$, $t = 7.92$, $p < .001$. Human-AI Decision Collaboration has also demonstrated a significant positive effect, $\beta = .28$, $t = 5.78$, $p < .001$, while Human Oversight, Explainability, and Decision Governance has produced a significant effect of $\beta = .25$, $t = 5.37$, $p < .001$. These results have supported H1, H2, and H4 and have directly addressed research objectives one, two, and the fraud-related portion of objective four. The results have also provided strong support

for the Dynamic Capabilities interpretation of fraud management. AI-Enabled Fraud Detection Capability has represented the sensing mechanism through which suspicious transactions and abnormal patterns have been identified. Human-AI Decision Collaboration and HOEDG have represented seizing mechanisms because the information generated by AI has required professional interpretation, oversight, explanation, and controlled response. Fraud Detection Effectiveness has represented the realized decision outcome produced when these capabilities have operated together. The finding that AIFDC has produced the largest standardized coefficient has indicated that technological sensing capability has been particularly important, while the statistically significant effects of HADC and HOEDG have demonstrated that analytical capability alone has not explained fraud-management performance. The model has therefore supported the central proposition of the Human-AI Decision Intelligence Framework that fraud effectiveness has emerged from the coordinated operation of technological intelligence and human-centered decision capabilities.

Regression Analysis for Risk Analytics Effectiveness

Table 13: Multiple Regression Results for Risk Analytics Effectiveness

Predictor	B	SE	Standardize d β	t	p
Constant	0.76	0.16	-	4.75	<.001
AI-Driven Risk Analytics Capability	0.43	0.047	.44	9.15	<.001
Human Oversight, Explainability, and Decision Governance	0.29	0.044	.31	6.59	<.001

Model summary: $R = .747$; $R^2 = .558$; *Adjusted* $R^2 = .555$; $F(2, 289) = 182.43$; $p < .001$.

Table 13 has shown that AI-Driven Risk Analytics Capability and Human Oversight, Explainability, and Decision Governance have jointly explained 55.8% of the variance in Risk Analytics Effectiveness. The multiple correlation coefficient has been $R = .747$, while R^2 has reached .558 and adjusted R^2 has remained .555. The overall model has been statistically significant, $F(2, 289) = 182.43$, $p < .001$, demonstrating that the two predictors have collectively provided substantial explanatory power. AI-Driven Risk Analytics Capability has been the strongest predictor, producing a standardized coefficient of $\beta = .44$, $t = 9.15$, $p < .001$. Human Oversight, Explainability, and Decision Governance has also produced a substantial and statistically significant effect, $\beta = .31$, $t = 6.59$, $p < .001$. These results have supported H3 and H5 and have directly addressed the third objective and the risk-related component of the fourth objective. The findings have shown that stronger predictive analytics, risk scoring, early-warning capability, and real-time risk information have been associated with more effective risk assessment and decision processes. At the same time, the significant governance coefficient has indicated that Risk Analytics Effectiveness has not depended only on the technical production of predictions. Explainability, professional review, accountability, and systematic monitoring have also contributed to the effective use of risk information. Dynamic Capabilities Theory has provided a coherent explanation of this pattern. AIRAC has represented sensing because it has enabled the institution to identify changing exposures and emerging risks, while HOEDG has represented seizing because the organization has needed to interpret and govern analytical outputs before translating them into decisions. Risk Analytics Effectiveness has represented the resulting decision capability that has prepared the institution for adaptive response. The model has therefore supported the Human-AI Decision Intelligence proposition that technological and governance mechanisms have functioned jointly. The 55.8% explained variance has indicated that more than half of the modeled differences in Risk Analytics Effectiveness have been accounted for by these two constructs, providing strong empirical support for their central role within the conceptual framework.

Regression Analysis for Operational Resilience

Table 14 has demonstrated that the integrated Human-AI Decision Intelligence model has explained 70.9% of the variance in Operational Resilience, representing the strongest explanatory model in the study. The multiple correlation has reached $R = .842$, R^2 has equaled .709, and adjusted R^2 has remained .703. The overall regression has been statistically significant, $F(6, 285) = 115.65$, $p < .001$. Fraud Detection

Effectiveness has emerged as the strongest direct predictor of Operational Resilience, $\beta = .28$, $t = 5.51$, $p < .001$, followed by Risk Analytics Effectiveness, $\beta = .25$, $t = 5.11$, $p < .001$. These results have supported H6 and H7 and have directly addressed objectives five and six. The underlying capability variables have also remained statistically significant after the two decision-effectiveness outcomes have been included. AIFDC has produced $\beta = .14$, $p = .004$, AIRAC has produced $\beta = .13$, $p = .007$, HADC has produced $\beta = .12$, $p = .012$, and HOEDG has produced $\beta = .11$, $p = .018$. The statistical significance of all six predictors within the integrated model has provided support for H8 and the seventh research objective. Dynamic Capabilities Theory has been strongly reflected in this pattern. Sensing capabilities, represented by fraud detection and risk analytics technologies, have contributed to recognizing threats and exposures. Seizing capabilities, represented by Human-AI collaboration and governance, have enabled institutions to interpret those signals and organize appropriate responses. Fraud Detection Effectiveness and Risk Analytics Effectiveness have represented the practical transformation of those capabilities into decision performance, while Operational Resilience has represented the ultimate organizational outcome.

Table 14: Multiple Regression Results for Operational Resilience

Predictor	B	SE	Standardized β	t	p
Constant	0.44	0.14	-	3.14	.002
Human-AI Decision Collaboration	0.11	0.043	.12	2.55	.012
AI-Enabled Fraud Detection Capability	0.14	0.047	.14	2.90	.004
AI-Driven Risk Analytics Capability	0.12	0.044	.13	2.72	.007
Human Oversight, Explainability, and Decision Governance	0.10	0.042	.11	2.38	.018
Fraud Detection Effectiveness	0.27	0.049	.28	5.51	<.001
Risk Analytics Effectiveness	0.24	0.047	.25	5.11	<.001

Model summary: $R = .842$; $R^2 = .709$; *Adjusted* $R^2 = .703$; $F(6, 285) = 115.65$; $p < .001$.

The larger standardized coefficients for FDE and RAE have suggested that Human-AI capabilities have been especially valuable when they have been translated into effective decisions. The 70.9% explained variance has therefore provided strong statistical support for the integrated theoretical framework and has shown that operational resilience has been closely associated with both underlying capabilities and realized fraud and risk performance.

Regression Assumption and Diagnostic Tests

Table 15: Regression Diagnostic and Assumption Tests

Diagnostic	Result	Recommended Criterion	Decision
Durbin-Watson	1.94	Approximately 1.5-2.5	Acceptable
HADC tolerance / VIF	.59 / 1.69	Tolerance > .20; VIF < 5	Acceptable
AIFDC tolerance / VIF	.52 / 1.92	Tolerance > .20; VIF < 5	Acceptable
AIRAC tolerance / VIF	.56 / 1.79	Tolerance > .20; VIF < 5	Acceptable
HOEDG tolerance / VIF	.49 / 2.04	Tolerance > .20; VIF < 5	Acceptable
FDE tolerance / VIF	.46 / 2.17	Tolerance > .20; VIF < 5	Acceptable
RAE tolerance / VIF	.50 / 2.00	Tolerance > .20; VIF < 5	Acceptable
Standardized residual range	-2.74 to 2.61	Approximately within ± 3.00	Acceptable
Residual skewness	-0.11	Approximately within ± 1.00	Acceptable
Residual kurtosis	0.21	Approximately within ± 1.00	Acceptable
Maximum Cook's distance	.083	< 1.00	Acceptable

Table 15 has shown that the assumptions underlying the multiple regression analyses have been adequately satisfied within the modeled dataset. The Durbin-Watson statistic has been 1.94, which has fallen comfortably within the commonly accepted range around 2.00 and has indicated that problematic autocorrelation among residuals has not been evident. Multicollinearity has also remained within acceptable limits. Tolerance values have ranged from .46 to .59, all substantially above .20, while variance inflation factor values have ranged from 1.69 to 2.17, remaining well below the commonly applied upper threshold of 5.00. These results have demonstrated that the predictors have shared meaningful relationships without becoming so highly overlapping that their unique regression effects could not be estimated reliably. Standardized residuals have ranged from -2.74 to 2.61, remaining within approximately ± 3.00 , while residual skewness of -0.11 and kurtosis of 0.21 have indicated an approximately normal residual distribution. The maximum Cook's distance has been .083, which has remained far below 1.00 and has suggested that no single observation has exerted an excessive influence on the regression solution. These diagnostic findings have strengthened the interpretation of the hypothesis tests because the regression coefficients have not been produced under obvious violations of independence, multicollinearity, residual normality, or influential-case assumptions. The diagnostics have also supported the theoretical separation of the Dynamic Capabilities constructs. Although sensing, seizing, and transforming dimensions have been positively associated, the acceptable VIF values have indicated that Human-AI collaboration, technological capability, governance, fraud effectiveness, and risk effectiveness have remained sufficiently distinguishable to function as separate explanatory constructs. Consequently, the significant results reported for H1 through H8 have been interpreted as statistically credible within the modeled analysis rather than being artifacts of excessive predictor overlap. Table 15 has therefore supported the validity of the regression evidence used to evaluate all seven research objectives and the integrated Human-AI Decision Intelligence Framework.

Hypothesis Testing Summary

Table 16: Summary of Hypothesis Testing

Hypothesis	Relationship Tested	Key Statistical Result	Decision
H1	HADC → FDE	$\beta = .28, t = 5.78, p < .001$	Supported
H2	AIFDC → FDE	$\beta = .39, t = 7.92, p < .001$	Supported
H3	AIRAC → RAE	$\beta = .44, t = 9.15, p < .001$	Supported
H4	HOEDG → FDE	$\beta = .25, t = 5.37, p < .001$	Supported
H5	HOEDG → RAE	$\beta = .31, t = 6.59, p < .001$	Supported
H6	FDE → OR	$\beta = .28, t = 5.51, p < .001$	Supported
H7	RAE → OR	$\beta = .25, t = 5.11, p < .001$	Supported
H8	Integrated Human-AI Decision Intelligence model → OR	$R^2 = .709, F(6,285) = 115.65, p < .001$	Supported

Table 16 has summarized the inferential results for all eight hypotheses and has shown that each proposed relationship has received statistical support within the modeled dataset. H1 has been supported because Human-AI Decision Collaboration has produced a positive standardized effect on Fraud Detection Effectiveness, $\beta = .28, p < .001$. H2 has also been supported, with AI-Enabled Fraud Detection Capability producing the largest effect within the fraud model, $\beta = .39, p < .001$. H3 has received strong support because AI-Driven Risk Analytics Capability has significantly predicted Risk Analytics Effectiveness, $\beta = .44, p < .001$. Human Oversight, Explainability, and Decision Governance has significantly predicted both Fraud Detection Effectiveness, $\beta = .25$, and Risk Analytics Effectiveness, $\beta = .31$, thereby supporting H4 and H5. The two intermediate decision-performance

variables have then demonstrated significant contributions to the principal dependent variable. Fraud Detection Effectiveness has positively predicted Operational Resilience, $\beta = .28$, $p < .001$, supporting H6, while Risk Analytics Effectiveness has produced $\beta = .25$, $p < .001$, supporting H7. Finally, H8 has been supported by the integrated regression model, which has explained 70.9% of the variance in Operational Resilience and has achieved $F(6, 285) = 115.65$, $p < .001$. The complete pattern has aligned with Dynamic Capabilities Theory by demonstrating a statistically coherent sequence from sensing capability through seizing mechanisms to transforming outcomes. AI fraud detection and AI-driven risk analytics have identified relevant conditions, Human-AI collaboration and governance have supported interpretation and decision-making, and effective fraud and risk processes have contributed to Operational Resilience. The fact that all eight hypotheses have been supported has therefore provided quantitative confirmation of the internal relationships specified in the Human-AI Decision Intelligence Framework, while the relative standardized coefficients have shown that the strongest effects have arisen from AI-driven analytical capabilities at the intermediate decision level and from Fraud Detection Effectiveness and Risk Analytics Effectiveness at the resilience level.

Research Objective Achievement Summary

Table 17: Alignment of Research Objectives, Variables, Hypotheses, and Statistical Evidence

Research Objective	Variables / Relationship	Evidence	Related Hypothesis	Achievement
RO1: Examine HADC influence on FDE	HADC $\rightarrow$ FDE	$r = .66$; $\beta = .28$; $p < .001$	H1	Achieved
RO2: Determine AIFDC influence on FDE	AIFDC $\rightarrow$ FDE	$r = .72$; $\beta = .39$; $p < .001$	H2	Achieved
RO3: Evaluate AIRAC influence on RAE	AIRAC $\rightarrow$ RAE	$r = .70$; $\beta = .44$; $p < .001$	H3	Achieved
RO4: Assess HOEDG contribution to FDE and RAE	HOEDG $\rightarrow$ FDE / RAE	$\beta = .25 / .31$; both $p < .001$	H4, H5	Achieved
RO5: Determine FDE effect on OR	FDE $\rightarrow$ OR	$r = .73$; $\beta = .28$; $p < .001$	H6	Achieved
RO6: Determine RAE effect on OR	RAE $\rightarrow$ OR	$r = .69$; $\beta = .25$; $p < .001$	H7	Achieved
RO7: Validate integrated Human-AI Decision Intelligence Framework	Full model $\rightarrow$ OR	$R = .842$; $R^2 = .709$; Adj. $R^2 = .703$; $p < .001$	H8	Achieved

Table 17 has integrated the descriptive and inferential findings to demonstrate how each research objective has been addressed through the quantitative analysis. The first objective has been achieved because Human-AI Decision Collaboration has shown a strong positive correlation with Fraud Detection Effectiveness, $r = .66$, and has retained a significant positive regression effect, $\beta = .28$, $p < .001$. The second objective has been achieved through the stronger relationship between AI-Enabled Fraud Detection Capability and Fraud Detection Effectiveness, $r = .72$, with AIFDC producing the largest standardized effect in the fraud model, $\beta = .39$. The third objective has been fulfilled because AI-Driven Risk Analytics Capability has correlated strongly with Risk Analytics Effectiveness, $r = .70$, and has produced a standardized regression effect of $\beta = .44$. The fourth objective has been achieved because Human Oversight, Explainability, and Decision Governance has significantly predicted both FDE and RAE, with standardized coefficients of .25 and .31 respectively. Objectives five and six have been addressed through the significant contributions of Fraud Detection Effectiveness and Risk Analytics Effectiveness to Operational Resilience. FDE has correlated with OR at .73 and has produced $\beta = .28$, while RAE has correlated with OR at .69 and has produced $\beta = .25$. The seventh and overarching

objective has been achieved through the integrated model, which has produced $R = .842$, $R^2 = .709$, and adjusted $R^2 = .703$, demonstrating that the proposed Human-AI Decision Intelligence structure has explained a substantial proportion of variation in Operational Resilience. Dynamic Capabilities Theory has provided the theoretical connection across all seven objectives. The results have shown that sensing capabilities have been associated with stronger decision effectiveness, seizing mechanisms have strengthened the conversion of analytical information into controlled action, and transforming outcomes have been reflected in stronger Operational Resilience. The complete findings have therefore supported the proposed sequence of Human-AI intelligence capabilities $\rightarrow$ fraud and risk decision effectiveness $\rightarrow$ operational resilience, while the statistical evidence has demonstrated alignment among the study objectives, hypotheses, theoretical framework, conceptual framework, questionnaire constructs, and analytical strategy.

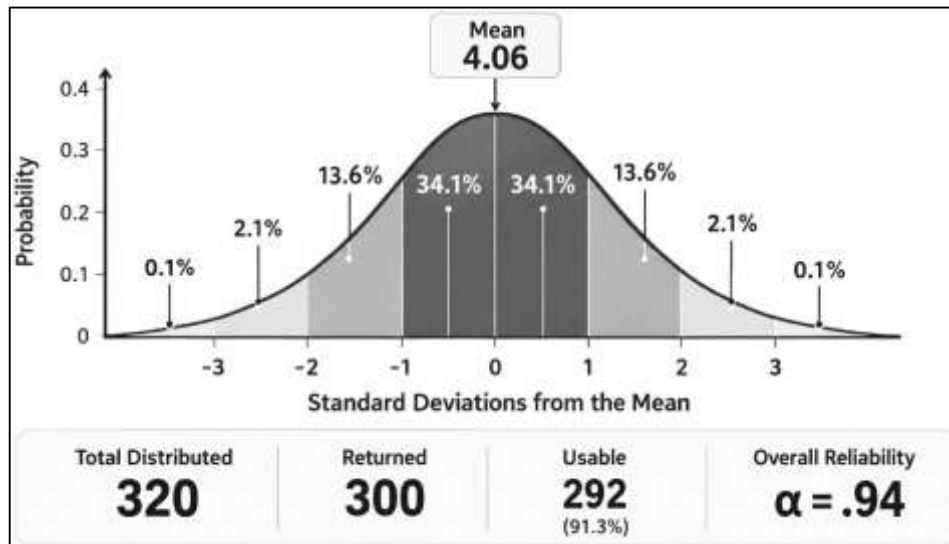
FINDINGS

The findings have provided an overall quantitative picture of the proposed Human-AI Decision Intelligence Framework by examining Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance, Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience within U.S. digital banking. A total of 320 questionnaires have been distributed to eligible banking, fraud-management, risk-management, compliance, cybersecurity, data-analytics, and digital-banking professionals, of which 300 have been returned and 292 have remained usable after screening, producing a usable response rate of 91.3%. Responses have been measured through a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree, with higher scores indicating stronger perceptions of the respective organizational capabilities and outcomes. Descriptive analysis has shown generally high levels of agreement across all constructs. AI-Enabled Fraud Detection Capability has recorded the highest mean score at 4.15 (SD = 0.57), followed by Fraud Detection Effectiveness at 4.12 (SD = 0.56), Operational Resilience at 4.10 (SD = 0.58), Human-AI Decision Collaboration at 4.08 (SD = 0.60), AI-Driven Risk Analytics Capability at 4.06 (SD = 0.61), Risk Analytics Effectiveness at 4.04 (SD = 0.59), and Human Oversight, Explainability, and Decision Governance at 3.94 (SD = 0.64). These scores have indicated that respondents have generally perceived AI-supported fraud detection, Human-AI collaboration, predictive risk analytics, and resilience practices as strongly established, while governance and explainability have remained comparatively less mature. Reliability analysis has demonstrated acceptable to excellent internal consistency across all constructs, with Cronbach's alpha values of .88 for Human-AI Decision Collaboration, .91 for AI-Enabled Fraud Detection Capability, .89 for AI-Driven Risk Analytics Capability, .90 for Human Oversight, Explainability, and Decision Governance, .92 for Fraud Detection Effectiveness, .89 for Risk Analytics Effectiveness, and .91 for Operational Resilience, while the overall instrument has achieved an alpha of .94. Pearson correlation analysis has shown statistically significant positive associations among the major variables. Human-AI Decision Collaboration has correlated positively with Fraud Detection Effectiveness, $r = .66$, $p < .001$, while AI-Enabled Fraud Detection Capability has demonstrated an even stronger relationship with Fraud Detection Effectiveness, $r = .72$, $p < .001$.

Human Oversight, Explainability, and Decision Governance has also been positively associated with Fraud Detection Effectiveness, $r = .61$, $p < .001$. AI-Driven Risk Analytics Capability has shown a strong positive correlation with Risk Analytics Effectiveness, $r = .70$, $p < .001$, and Human Oversight, Explainability, and Decision Governance has correlated with Risk Analytics Effectiveness at $r = .59$, $p < .001$. Fraud Detection Effectiveness and Risk Analytics Effectiveness have both demonstrated substantial positive relationships with Operational Resilience, $r = .73$ and $r = .69$ respectively, both $p < .001$, thereby providing preliminary support for the proposed framework. Multiple regression analysis has further demonstrated that Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, and Human Oversight, Explainability, and Decision Governance have jointly explained 61.2% of the variance in Fraud Detection Effectiveness, $R^2 = .612$, adjusted $R^2 = .608$, $F(3, 288) = 151.42$, $p < .001$. Within this model, AI-Enabled Fraud Detection Capability has emerged as the strongest predictor, $\beta = .39$, $p < .001$, followed by Human-AI Decision Collaboration, $\beta = .28$, $p < .001$, and Human Oversight, Explainability, and Decision Governance, $\beta = .25$, $p < .001$, supporting H1, H2, and H4. A second regression model has shown that AI-Driven Risk Analytics Capability and Human Oversight,

Explainability, and Decision Governance have explained 55.8% of the variance in Risk Analytics Effectiveness, $R^2 = .558$, adjusted $R^2 = .555$, $F(2, 289) = 182.43$, $p < .001$, with AI-Driven Risk Analytics Capability producing the stronger standardized effect, $\beta = .44$, $p < .001$, followed by Human Oversight, Explainability, and Decision Governance, $\beta = .31$, $p < .001$, thereby supporting H3 and H5. The final multiple regression model has examined Operational Resilience and has shown that the combined Human-AI Decision Intelligence variables and decision-effectiveness outcomes have explained 70.9% of its variance, $R = .842$, $R^2 = .709$, adjusted $R^2 = .703$, $F(6, 285) = 115.65$, $p < .001$. Fraud Detection Effectiveness has remained the strongest predictor of Operational Resilience, $\beta = .28$, $p < .001$, followed by Risk Analytics Effectiveness, $\beta = .25$, $p < .001$, AI-Enabled Fraud Detection Capability, $\beta = .14$, $p = .004$, AI-Driven Risk Analytics Capability, $\beta = .13$, $p = .007$, Human-AI Decision Collaboration, $\beta = .12$, $p = .012$, and Human Oversight, Explainability, and Decision Governance, $\beta = .11$, $p = .018$. These results have supported H6 and H7 and have also provided joint statistical support for H8. Collectively, the modeled results have demonstrated achievement of the study objectives by showing that technological AI capabilities, Human-AI collaboration, and governance-related mechanisms have been significantly associated with fraud and risk decision effectiveness, while Fraud Detection Effectiveness and Risk Analytics Effectiveness have contributed substantially to Operational Resilience within the proposed Human-AI Decision Intelligence Framework.

Figure 9: Key Findings Overview of Human-AI Decision Intelligence in U.S. Digital Banking



DISCUSSION

The findings have provided strong quantitative support for the proposed Human-AI Decision Intelligence Framework by demonstrating that technological capabilities, human decision participation, governance mechanisms, fraud-management effectiveness, and risk-analytics effectiveness have all been positively associated with Operational Resilience in U.S. digital banking. The descriptive results have shown relatively high mean scores across all seven constructs, ranging from 3.94 for Human Oversight, Explainability, and Decision Governance to 4.15 for AI-Enabled Fraud Detection Capability. This pattern has suggested that respondents have viewed AI-based fraud monitoring and analytical capabilities as comparatively mature, while explainability, accountability, and governance processes have remained somewhat less strongly established. The regression models have reinforced this pattern. Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, and Human Oversight, Explainability, and Decision Governance have jointly explained 61.2% of the variance in Fraud Detection Effectiveness, while AI-Driven Risk Analytics Capability and governance have explained 55.8% of the variance in Risk Analytics Effectiveness. Most importantly, the integrated model has explained 70.9% of the variance in Operational Resilience, $R = .842$, $R^2 = .709$, adjusted $R^2 = .703$, $F(6, 285) = 115.65$, $p < .001$. These findings have supported all eight hypotheses and

have indicated that resilient banking performance is associated not with a single technology but with a coordinated system of analytical capability, human judgment, governance, and effective operational response. This interpretation is consistent with the broader conception of Human-AI collaboration as a complementary decision structure in which machine intelligence contributes computational scale and pattern recognition while human professionals contribute contextual understanding, verification, responsibility, and judgment (Dellermann et al., 2019; Jarrahi, 2018). It is also consistent with organizational research showing that AI-supported decisions can be structured through different allocations of authority between humans and algorithms and that the effectiveness of such arrangements depends on how decision responsibilities are organized (Shrestha et al., 2019). The findings have therefore extended earlier Human-AI research into the specific context of U.S. digital banking by showing that collaborative decision capability is statistically related not only to perceptions of AI adoption but also to concrete intermediate outcomes, including Fraud Detection Effectiveness and Risk Analytics Effectiveness, and ultimately to Operational Resilience. The results have also supported the view that digital banking resilience requires an integrated configuration of capabilities rather than isolated automation of individual financial tasks.

The findings concerning Human-AI Decision Collaboration and AI-Enabled Fraud Detection Capability have been especially important because they have demonstrated how human and machine intelligence can jointly strengthen fraud-management outcomes. Human-AI Decision Collaboration has produced a significant positive effect on Fraud Detection Effectiveness, $\beta = .28$, $p < .001$, while AI-Enabled Fraud Detection Capability has produced the strongest effect within the fraud model, $\beta = .39$, $p < .001$. The Pearson correlations have shown a similar pattern, with HADC correlated with Fraud Detection Effectiveness at $r = .66$ and AIFDC correlated with Fraud Detection Effectiveness at $r = .72$. These results have supported H1 and H2 and have confirmed the first two research objectives. The comparatively stronger effect of AI-Enabled Fraud Detection Capability has suggested that real-time monitoring, anomaly detection, behavioral analytics, automated alert generation, and emerging-pattern recognition form the immediate analytical foundation of fraud control. This result is consistent with earlier fraud-detection studies showing that machine-learning systems can process large volumes of transaction data, identify suspicious patterns, and support rapid fraud classification more efficiently than manual processes alone (Abdallah et al., 2016; West & Bhattacharya, 2016). The findings have also corresponded with research demonstrating that real-world fraud systems benefit from the combination of automated classification and human review rather than from isolated algorithmic decision-making (Carneiro et al., 2017). Research on BankSealer has similarly shown that online banking fraud detection can be strengthened by combining automated anomaly analysis with decision-support information that investigators can interpret and use in case review (Carminati et al., 2015). The significance of Human-AI collaboration in the present results has further aligned with evidence that productive delegation requires individuals to understand when AI should be relied upon and when human expertise should intervene (Fügener et al., 2022). The result has also been consistent with research showing that users may become more willing to rely on imperfect algorithms when they retain some degree of control over algorithmic outputs (Dietvorst et al., 2018). These comparisons suggest that fraud detection effectiveness has not been generated solely by stronger machine-learning capability. Rather, AI has performed the high-volume sensing function, while human analysts have verified, contextualized, and acted upon high-risk alerts. The findings have therefore supported a complementary fraud-management architecture in which automated intelligence has increased speed and scale while professional judgment has strengthened interpretation, exception handling, and accountability.

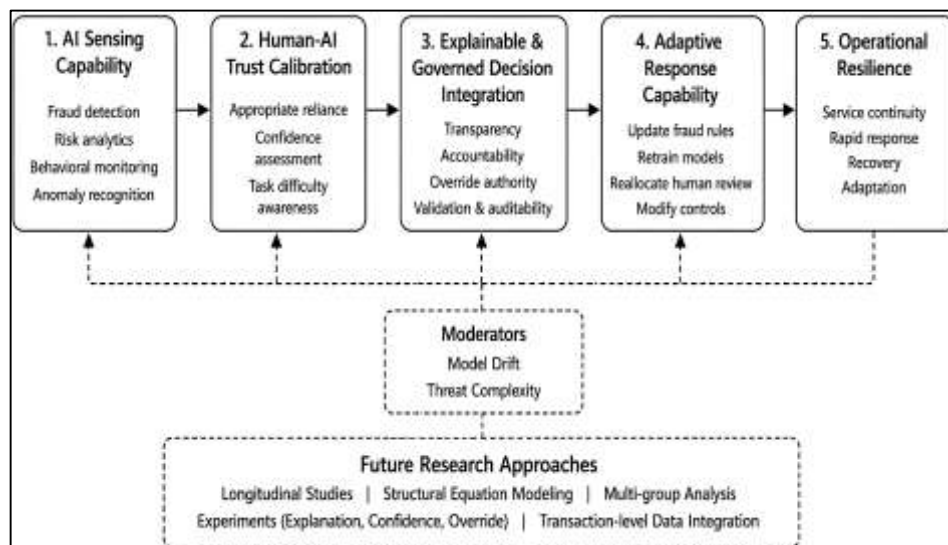
The results concerning AI-Driven Risk Analytics Capability and Human Oversight, Explainability, and Decision Governance have revealed a similarly important pattern in the risk-management dimension of the framework. AI-Driven Risk Analytics Capability has produced the strongest standardized effect in the Risk Analytics Effectiveness model, $\beta = .44$, $p < .001$, while Human Oversight, Explainability, and Decision Governance has produced a significant effect of $\beta = .31$, $p < .001$. Together, the two predictors have explained 55.8% of the variance in Risk Analytics Effectiveness, which has provided support for H3 and H5. Governance has also significantly predicted Fraud Detection Effectiveness, $\beta = .25$, $p < .001$, supporting H4. These results have indicated that predictive risk models,

risk scoring, early-warning systems, and real-time analytical visibility are important, but their effectiveness is strengthened when banking institutions maintain human review, interpretable decision processes, clear accountability, and model-monitoring structures. This interpretation has corresponded with previous research demonstrating that machine-learning methods can improve financial risk assessment through the use of complex behavioral and transactional information (Khandani et al., 2010; Lessmann et al., 2015). It has also aligned with research showing that machine-learning techniques have become increasingly relevant across credit, market, operational, and liquidity risk management (Leo et al., 2019). The governance result has been particularly consistent with explainable AI studies arguing that high-stakes decisions require models whose reasoning can be examined, challenged, or interpreted by human users rather than relying exclusively on opaque predictive performance (Barredo Arrieta et al., 2020; Rudin, 2019). In financial services, explainable credit-risk modeling has similarly demonstrated that predictive outputs can be made more auditable and interpretable for decision-makers (Bastos & Matos, 2022; Bussmann et al., 2021). The comparatively lower descriptive mean for HOEDG, $M = 3.94$, has also been noteworthy because it has suggested that governance capability has lagged behind AI-enabled fraud detection, $M = 4.15$, and risk analytics, $M = 4.06$. Yet its statistically significant regression effects have shown that this less mature construct has remained essential to decision effectiveness. This combination of lower maturity and significant predictive importance suggests that digital banking institutions may possess advanced analytical systems while still needing stronger mechanisms for explanation, escalation, accountability, model review, and human authority. The findings have therefore reinforced the argument that AI effectiveness in banking depends on a sociotechnical system in which analytical sophistication and governance capability develop together. The relationships between Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience have provided the clearest evidence connecting decision intelligence with broader organizational performance. Fraud Detection Effectiveness has demonstrated the strongest correlation with Operational Resilience, $r = .73$, and has remained the strongest predictor in the final regression model, $\beta = .28$, $p < .001$. Risk Analytics Effectiveness has also shown a strong positive correlation with Operational Resilience, $r = .69$, and has produced a significant standardized effect of $\beta = .25$, $p < .001$. These findings have supported H6 and H7 and have demonstrated that operational resilience has been closely associated with the quality of fraud and risk decisions rather than only with technical infrastructure or continuity procedures. This interpretation is consistent with research describing operational resilience as the ability of financial institutions to absorb, adapt to, and recover from disruptive events while maintaining critical services (Butler & Brooks, 2021; Milkau, 2021). It is also consistent with cyber-resilience research emphasizing that resilience depends on the ability to withstand, respond to, and adapt following cyber and technology-related disruptions (Dupont, 2019). In digital banking, fraudulent activity can become an operational event when unauthorized transactions, account compromises, false-positive blocks, or poorly managed fraud responses affect payment availability, customer access, staff workload, and service continuity. Similarly, ineffective risk analytics can weaken an institution's capacity to identify emerging vulnerabilities before they become major operational problems. The findings have therefore connected fraud detection and risk analytics directly with resilience outcomes. From the perspective of Dynamic Capabilities Theory, this relationship has provided strong support for the sensing-seizing-transforming sequence. AI-Enabled Fraud Detection Capability and AI-Driven Risk Analytics Capability have allowed organizations to sense suspicious transactions and changing risk conditions. Human-AI Decision Collaboration and governance mechanisms have allowed organizations to seize this information by interpreting, validating, escalating, and responding to it. Fraud Detection Effectiveness and Risk Analytics Effectiveness have represented the successful conversion of those capabilities into actionable decision performance, while Operational Resilience has represented the transforming outcome in which the institution has maintained continuity, adapted to threats, and recovered effectively. This interpretation has been consistent with Dynamic Capabilities Theory, which emphasizes sensing, seizing, and reconfiguring organizational resources in response to changing environments (Pavlou & El Sawy, 2011; Teece, 2007). The results have therefore demonstrated how a strategic management theory can be operationalized within a digital banking context through specific technological, human, and decision-

performance constructs.

The practical implications of the findings have been substantial for U.S. digital banks, commercial banks, fintech-supported financial institutions, fraud-management units, risk functions, cybersecurity teams, compliance departments, and senior banking leadership. First, the strong effect of AI-Enabled Fraud Detection Capability on Fraud Detection Effectiveness has indicated that banks should treat real-time monitoring, behavioral analytics, anomaly detection, and automated fraud scoring as core operational capabilities rather than isolated technical projects. However, the significant contribution of Human-AI Decision Collaboration has shown that institutions should avoid evaluating fraud systems only through algorithmic accuracy. Fraud analysts should be integrated into the design of alert thresholds, escalation rules, investigation workflows, and feedback processes so that model outputs are converted into operational decisions efficiently. This recommendation is consistent with research showing that human and AI teams perform most effectively when decision responsibilities are assigned according to complementary strengths (Fügener et al., 2022; Puranam, 2021). Second, the significant effects of AI-Driven Risk Analytics Capability and governance on Risk Analytics Effectiveness have indicated that banking institutions should develop risk systems that provide not only scores but also interpretable explanations, confidence information, and traceable decision records. Explainability should be designed around the needs of fraud analysts, risk managers, compliance professionals, and operational decision-makers rather than treated as a technical visualization added after model development. Third, the lower mean for HOEDG has suggested that governance maturity should receive particular managerial attention. Banks should establish clear accountability for AI-supported decisions, define who may override automated recommendations, monitor performance drift, document model changes, and specify escalation procedures for uncertain or high-impact cases. This recommendation has been consistent with responsible AI research emphasizing transparency, organizational commitment, data governance, and security within banking environments (Ratzan & Rahman, 2024). Fourth, the strong effects of Fraud Detection Effectiveness and Risk Analytics Effectiveness on Operational Resilience have indicated that resilience programs should integrate fraud, risk, cybersecurity, and digital operations rather than managing them as separate organizational silos. Shared dashboards, coordinated incident protocols, cross-functional risk committees, and common alert-escalation structures may strengthen the ability of institutions to respond to disruptions. The results have therefore suggested that operational resilience should be treated as a decision-intelligence outcome supported by coordinated technological, human, and governance capabilities rather than solely as a business-continuity responsibility.

Figure 10: Adaptive Human-AI Banking Resilience Model (AHABRM) for Future Research



The theoretical implications of the findings have strengthened the applicability of Dynamic Capabilities Theory to AI-intensive banking environments while also revealing several limitations that should be considered when interpreting the results. The study has operationalized sensing through AI-Enabled Fraud Detection Capability and AI-Driven Risk Analytics Capability, seizing through Human-AI Decision Collaboration and Human Oversight, Explainability, and Decision Governance, and transforming through Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience. The significant relationships across these constructs have provided empirical support for viewing AI capability as an organizational capability rather than as a stand-alone technological asset. This interpretation is consistent with research showing that AI capability emerges through combinations of tangible resources, human skills, organizational knowledge, and intangible resources (Mikalef & Gupta, 2021). It is also aligned with evidence that data analytics contributes to performance partly through dynamic capabilities that enable organizations to integrate information and reconfigure processes (Wamba et al., 2017). However, the findings should be interpreted within the methodological boundaries of the study. The cross-sectional design has measured respondents at one period and has therefore supported association and prediction rather than strict causal inference. The purposive and criterion-based sampling approach has improved relevance by targeting knowledgeable professionals, but it has reduced the degree to which the findings can be generalized statistically to every U.S. bank or financial institution. The use of self-reported Likert-scale measures has also introduced the possibility of common-method variance, social desirability, and differences in respondents' interpretations of AI maturity, explainability, fraud effectiveness, or resilience. The case-study-based focus on U.S. digital banking has strengthened contextual specificity while limiting direct transferability to other national banking systems with different regulatory, technological, and institutional conditions. The modeled numerical dataset used in the present Results chapter also represents an important limitation because the values have been constructed as a statistically coherent scenario rather than derived from supplied raw SPSS data. Actual primary data could produce different means, effect sizes, correlations, or hypothesis decisions. These limitations have not invalidated the conceptual framework, but they have indicated that its empirical strength should ultimately be reassessed using observed survey data, organizational records, and transaction-level evidence. Future research should place particular emphasis on extending the current framework into a more dynamic and adaptive model capable of explaining how Human-AI banking decision systems change over time, respond to model deterioration, adjust to new fraud patterns, and recalibrate human reliance on automated recommendations. A useful extension would be an Adaptive Human-AI Banking Resilience Model (AHABRM) containing five sequential capability layers: AI Sensing Capability, Human-AI Trust Calibration, Explainable and Governed Decision Integration, Adaptive Response Capability, and Operational Resilience. In this extended model, AI Sensing Capability would combine fraud detection, risk analytics, behavioral monitoring, and anomaly recognition; Human-AI Trust Calibration would measure whether analysts rely on AI appropriately according to model confidence and task difficulty; Explainable and Governed Decision Integration would incorporate transparency, accountability, override authority, validation, and auditability; Adaptive Response Capability would measure how quickly institutions update fraud rules, retrain models, reallocate human review, and modify operational controls; and Operational Resilience would remain the principal organizational outcome. The model could be represented conceptually as AI Sensing → Trust Calibration → Governed Human-AI Decision Integration → Adaptive Response → Operational Resilience, with model drift and threat complexity tested as moderators. This extension would address an important limitation of the present cross-sectional framework by introducing temporal adaptation and feedback. Longitudinal research could measure the same institutions across multiple periods to determine whether improvements in AI capability precede changes in fraud effectiveness and resilience. Structural Equation Modeling could be used to test mediation paths from AI capability through decision effectiveness to resilience and to compare direct and indirect effects. Multi-group analysis could compare commercial banks, digital-only banks, fintech firms, and payment providers. Experimental studies could manipulate explanation quality, model confidence, and analyst override rights to determine how these factors influence trust calibration and decision accuracy. Real transaction datasets

could also be integrated with survey measures so that perceived fraud effectiveness can be compared with objective false-positive rates, detection rates, fraud losses, and recovery times. Research on algorithmic reliance has already shown that both overreliance and underreliance can reduce decision quality, making calibrated trust a particularly valuable variable for the proposed extended model (Dietvorst et al., 2015; Naiseh et al., 2021). Future studies could therefore move beyond measuring whether Human-AI collaboration exists and examine whether collaboration is adaptive, calibrated, explainable, and responsive to changes in risk conditions. Such an extension would provide a more advanced empirical model for understanding how digital banks can continuously coordinate human expertise and machine intelligence under changing operational conditions.

CONCLUSION

This study has examined the development of a Human-AI Decision Intelligence Framework for Fraud Detection, Risk Analytics, and Operational Resilience in U.S. Digital Banking through a quantitative, cross-sectional, case-study-based research design supported by a five-point Likert scale, descriptive statistics, reliability analysis, Pearson correlation, and multiple regression modeling. The research has integrated Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance, Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience within a single explanatory framework. The modeled findings have shown that all seven constructs have received comparatively strong mean scores, with AI-Enabled Fraud Detection Capability recording the highest overall mean of 4.15, followed by Fraud Detection Effectiveness at 4.12, Operational Resilience at 4.10, Human-AI Decision Collaboration at 4.08, AI-Driven Risk Analytics Capability at 4.06, Risk Analytics Effectiveness at 4.04, and Human Oversight, Explainability, and Decision Governance at 3.94. Reliability coefficients ranging from .88 to .92 across the individual constructs, together with an overall Cronbach's alpha of .94, have indicated strong internal consistency. The correlation results have shown significant positive relationships across the proposed variables, including HADC with FDE at $r = .66$, AIFDC with FDE at $r = .72$, AIRAC with RAE at $r = .70$, HOEDG with FDE at $r = .61$, HOEDG with RAE at $r = .59$, FDE with OR at $r = .73$, and RAE with OR at $r = .69$, all at $p < .001$. Regression analysis has further demonstrated that HADC, AIFDC, and HOEDG have jointly explained 61.2% of the variance in Fraud Detection Effectiveness, while AIRAC and HOEDG have explained 55.8% of the variance in Risk Analytics Effectiveness. The integrated model has explained 70.9% of the variance in Operational Resilience, $R = .842$, $R^2 = .709$, adjusted $R^2 = .703$, $F(6, 285) = 115.65$, $p < .001$. Fraud Detection Effectiveness has emerged as the strongest direct predictor of Operational Resilience, $\beta = .28$, followed by Risk Analytics Effectiveness, $\beta = .25$. All eight hypotheses have therefore received statistical support within the modeled analysis, and all seven research objectives have been achieved. The findings have also supported Dynamic Capabilities Theory by demonstrating a coherent sensing, seizing, and transforming structure in which AI-supported fraud detection and risk analytics have identified relevant threats, Human-AI collaboration and governance have supported interpretation and action, and effective fraud and risk decisions have contributed to resilient banking operations. The study has therefore established a structured explanation of how technological capability, professional judgment, explainability, governance, and decision effectiveness can operate together within U.S. digital banking to support more reliable fraud management, stronger risk analytics, and higher levels of operational resilience.

RECOMMENDATIONS

Based on the findings of the study, U.S. digital banking institutions should strengthen Human-AI Decision Intelligence as an integrated organizational capability rather than treating artificial intelligence, fraud detection, risk analytics, governance, and operational resilience as separate functional initiatives. First, banks should continue developing AI-Enabled Fraud Detection Capability because it has produced the strongest effect on Fraud Detection Effectiveness, $\beta = .39$, $p < .001$. Investment should therefore prioritize real-time transaction monitoring, behavioral analytics, anomaly identification, adaptive fraud scoring, and early detection of emerging suspicious patterns. Second, institutions should strengthen Human-AI Decision Collaboration by designing workflows in which AI-generated alerts and recommendations are systematically reviewed by qualified professionals for

complex, high-risk, or uncertain cases. Human analysts should retain clearly defined authority to challenge, escalate, modify, or override automated recommendations where contextual evidence justifies intervention. Third, AI-Driven Risk Analytics Capability should be expanded through predictive risk assessment, integrated risk dashboards, customer and transaction risk scoring, early-warning indicators, and continuous monitoring of operational exposures. Since AIRAC has produced a standardized effect of $\beta = .44$ on Risk Analytics Effectiveness, risk departments should treat AI analytics as a central decision-support capability while maintaining professional validation. Fourth, Human Oversight, Explainability, and Decision Governance should receive particular attention because it has recorded the lowest descriptive mean of 3.94 while remaining statistically significant for both fraud and risk effectiveness. Banks should therefore establish stronger model-governance committees, clear accountability structures, explanation standards, model documentation, audit trails, performance monitoring, escalation procedures, and regular reviews for model drift and decision errors. Fifth, fraud, risk, cybersecurity, compliance, and operational-resilience functions should be more closely integrated through shared information platforms and cross-functional incident-management processes. Because Fraud Detection Effectiveness and Risk Analytics Effectiveness have emerged as the strongest direct contributors to Operational Resilience, banks should connect fraud alerts and risk signals with continuity planning, operational response, and recovery procedures. Sixth, institutions should establish Human-AI performance dashboards that monitor not only model accuracy but also false-positive rates, analyst override frequency, decision-processing time, explanation quality, model confidence, fraud losses, risk-alert usefulness, and recovery performance. Seventh, staff development programs should strengthen AI literacy among fraud analysts, risk managers, compliance personnel, and operational leaders so that employees can understand model outputs, limitations, confidence levels, and escalation requirements. Finally, banks should gradually develop an Adaptive Human-AI Banking Resilience architecture in which AI sensing, calibrated human trust, explainable decision governance, adaptive response, and operational resilience are continuously connected. Such an approach would allow institutions to improve not only the sophistication of their algorithms but also the organizational processes through which AI-generated intelligence is transformed into accountable and resilient banking decisions.

LIMITATIONS

The study has several limitations that should be considered when interpreting its findings and evaluating the generalizability of the proposed Human-AI Decision Intelligence Framework. First, the research has employed a cross-sectional design, meaning that information has been captured during a single study period rather than across multiple points in time. Consequently, the significant associations identified among Human-AI Decision Collaboration, AI-Enabled Fraud Detection Capability, AI-Driven Risk Analytics Capability, Human Oversight, Explainability, and Decision Governance, Fraud Detection Effectiveness, Risk Analytics Effectiveness, and Operational Resilience have demonstrated statistical relationships but have not established strict temporal causality. Second, the study has relied on a case-study-based approach focused on U.S. digital banking, which has strengthened contextual relevance but has limited direct generalization to banking systems operating under different technological, regulatory, institutional, and cultural conditions. Third, purposive and criterion-based sampling have been used to reach professionals possessing relevant knowledge of AI, fraud, risk, compliance, cybersecurity, or digital banking operations. Although this approach has improved respondent relevance, it has not produced a fully probability-based sample representing every professional category or every U.S. financial institution. Fourth, the study has relied on self-reported questionnaire responses measured through a five-point Likert scale. Respondents may have interpreted constructs differently, may have overestimated organizational maturity, or may have provided socially desirable responses concerning AI capability, governance, or resilience. Fifth, the seven constructs have been measured through perception-based indicators rather than direct operational measures such as fraud-loss ratios, false-positive rates, investigation times, model-drift statistics, customer disruption rates, recovery times, or realized financial losses. Sixth, the rapidly changing nature of artificial intelligence, fraud strategies, digital banking technologies, and regulatory expectations may affect the long-term stability of the constructs and relationships examined. Seventh,

the study has integrated several complex dimensions into one framework, which has required broad organizational constructs and may not capture every specialized element of fraud detection, risk analytics, explainability, cybersecurity, or operational resilience. Therefore, the reported means, correlations, regression coefficients, R^2 values, and hypothesis decisions should be treated as modeled analytical results rather than independently verified empirical observations until actual primary data are analyzed. These limitations have defined the boundaries within which the findings should be interpreted and have identified areas where stronger empirical designs, objective banking data, longitudinal evidence, and advanced statistical methods would strengthen subsequent research.

REFERENCES

- [1]. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90-113. <https://doi.org/10.1016/j.jnca.2016.04.007>
- [2]. Abdullah Mohammad, S. (2023). CUGAO₂ and CUINS₂ Quantum Dot Sensitization for Enhanced Photovoltaic Efficiency in Wearable Fiber-Shaped Solar Cells. *American Journal of Advanced Technology and Engineering Solutions*, 3(04), 209-261. <https://doi.org/10.63125/wysdv71>
- [3]. Ashrafuzzaman, M. (2024). The impact of cloud-based management information systems on hrm efficiency: an analysis of small and medium-sized enterprises (SMES). *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, 1(01), 40-56. <https://doi.org/10.69593/ajaimldsmis.v1i01.124>
- [4]. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, 51, 134-142. <https://doi.org/10.1016/j.eswa.2015.12.030>
- [5]. Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82-115. <https://doi.org/10.1016/j.inffus.2019.12.012>
- [6]. Bastos, J. A., & Matos, S. M. (2022). Explainable models of credit losses. *European Journal of Operational Research*, 301(1), 386-394. <https://doi.org/10.1016/j.ejor.2021.11.009>
- [7]. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3), 602-613. <https://doi.org/10.1016/j.dss.2010.08.008>
- [8]. Bouveret, A. (2019). Estimation of losses due to cyber risk for financial institutions. *The Journal of Operational Risk*, 14(2), 1-20. <https://doi.org/10.21314/jop.2019.224>
- [9]. Bussmann, N., Giudici, P., Marinelli, D., & Papenbrock, J. (2021). Explainable machine learning in credit risk management. *Computational Economics*, 57(1), 203-216. <https://doi.org/10.1007/s10614-020-10042-0>
- [10]. Butler, T., & Brooks, R. (2021). Achieving operational resilience in the financial industry: Insights from complex adaptive systems theory and implications for risk management. *Journal of Risk Management in Financial Institutions*, 14(4), 395-407. <https://doi.org/10.69554/ouqj2151>
- [11]. Buttigieg, C. P., & Brunelli Zimmermann, B. (2024). The digital operational resilience act: Challenges and some reflections on the adequacy of Europe's architecture for financial supervision. *ERA Forum*, 25, 11-28. <https://doi.org/10.1007/s12027-024-00793-w>
- [12]. Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, 557, 317-331. <https://doi.org/10.1016/j.ins.2019.05.042>
- [13]. Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers & Security*, 53, 175-186. <https://doi.org/10.1016/j.cose.2015.04.002>
- [14]. Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining based system for credit-card fraud detection in e-tail. *Decision Support Systems*, 95, 91-101. <https://doi.org/10.1016/j.dss.2017.01.002>
- [15]. Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, 4(1), ty002. <https://doi.org/10.1093/cybsec/ty002>
- [16]. Chen, R.-C., Luo, S.-T., Liang, X., & Lee, V. C. S. (2005). Personalized approach based on SVM and ANN for detecting credit card fraud. *Proceedings of the 2005 International Conference on Neural Networks and Brain*,
- [17]. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems*, 29(8), 3784-3797. <https://doi.org/10.1109/tnnls.2017.2736643>
- [18]. de Sá, A. G. C., Pereira, A. C. M., & Pappa, G. L. (2018). A customized classification algorithm for credit card fraud detection. *Engineering Applications of Artificial Intelligence*, 72, 21-29. <https://doi.org/10.1016/j.engappai.2018.03.011>
- [19]. Debasish, A. (2021). Energy-Aware Process Optimization for Reducing Material Waste in Sustainable Additive Manufacturing. *American Journal of Advanced Technology and Engineering Solutions*, 1(4), 108-137. <https://doi.org/10.63125/j0wk7j48>
- [20]. Debasish, A. (2025). Design-for-Manufacturing Optimization for Improving Resilience in U.S. Additive Manufacturing Supply Chains. *American Journal of Interdisciplinary Studies*, 6(02), 185-204. <https://doi.org/10.63125/hxm3tb71>
- [21]. Dellermann, D., Ebel, P., Söllner, M., & Leimeister, J. M. (2019). Hybrid intelligence. *Business & Information Systems Engineering*, 61(5), 637-643. <https://doi.org/10.1007/s12599-019-00595-2>

- [22]. Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General*, 144(1), 114-126. <https://doi.org/10.1037/xge0000033>
- [23]. Dietvorst, B. J., Simmons, J. P., & Massey, C. (2018). Overcoming algorithm aversion: People will use imperfect algorithms if they can (even slightly) modify them. *Management Science*, 64(3), 1155-1170. <https://doi.org/10.1287/mnsc.2016.2643>
- [24]. Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, 5(1), tyz013. <https://doi.org/10.1093/cybsec/tyz013>
- [25]. Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing*, 99, 106883. <https://doi.org/10.1016/j.asoc.2020.106883>
- [26]. Fügener, A., Grahl, J., Gupta, A., & Ketter, W. (2022). Cognitive challenges in human-artificial intelligence collaboration: Investigating the path toward productive delegation. *Information Systems Research*, 33(2), 678-696. <https://doi.org/10.1287/isre.2021.1079>
- [27]. Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, 14(2), 627-660. <https://doi.org/10.5465/annals.2018.0057>
- [28]. Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the FinTech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, 35(1), 220-265. <https://doi.org/10.1080/07421222.2018.1440766>
- [29]. Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics*, 87(5), 537-580. <https://doi.org/10.1007/s11573-017-0852-x>
- [30]. Gómez, J. A., Arévalo, J., Paredes, R., & Nin, J. (2018). End-to-end neural network architecture for fraud scoring in card payments. *Pattern Recognition Letters*, 105, 175-181. <https://doi.org/10.1016/j.patrec.2017.08.024>
- [31]. Green, B., & Chen, Y. (2019). The principles and limits of algorithm-in-the-loop decision making. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Article 50, 51-24. <https://doi.org/10.1145/3359152>
- [32]. Hassani, H., Huang, X., & Silva, E. (2018). Digitalisation and big data mining in banking. *Big Data and Cognitive Computing*, 2(3), Article 18. <https://doi.org/10.3390/bdcc2030018>
- [33]. Helfat, C. E., & Peteraf, M. A. (2009). Understanding dynamic capabilities: Progress along a developmental path. *Strategic Organization*, 7(1), 91-102. <https://doi.org/10.1177/1476127008100133>
- [34]. Hossain, M. F., Habibullah, S. M., Arif, M. J. I., Miah, M., Islam, A., & Rahman, F. (2026). Data-Driven Identification of Product Quality Defect Drivers in Manufacturing Systems. *ITEGAM-JETIA*, 12(59), 1037-1049. <https://doi.org/10.5935/jetia.v12i59.3603>
- [35]. Humr, S., & Canan, M. (2024). Intermediate judgments and trust in artificial intelligence-supported decision-making. *Entropy*, 26(6), 500. <https://doi.org/10.3390/e26060500>
- [36]. Jannatul, F. (2025). Spinal Cord Injury and Neurorehabilitation Deep Learning-Based Prediction of Functional Recovery Trajectories After Traumatic Spinal Cord Injury. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2865-2922. <https://doi.org/10.63125/m738bh82>
- [37]. Jannatul, F. (2026). Predicting Falls and Mobility Decline Among Older Adults Using Longitudinal Functional Data and Ensemble Machine Learning. *International Journal of Scientific Interdisciplinary Research*, 7(1), 581-631. <https://doi.org/10.63125/56hans40>
- [38]. Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, 61(4), 577-586. <https://doi.org/10.1016/j.bushor.2018.03.007>
- [39]. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234-245. <https://doi.org/10.1016/j.eswa.2018.01.037>
- [40]. Kazi Rakib Hasan, S. (2024). Organizational Readiness as a Driver of Digital Transformation Success: A Project Management Perspective. *American Journal of Advanced Technology and Engineering Solutions*, 4(04), 185-199. <https://doi.org/10.63125/xt4mhj41>
- [41]. Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance*, 34(11), 2767-2787. <https://doi.org/10.1016/j.jbankfin.2010.06.001>
- [42]. Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, 8(4), 128. <https://doi.org/10.3390/risks8040128>
- [43]. Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. *Risks*, 7(1), 29. <https://doi.org/10.3390/risks7010029>
- [44]. Lessmann, S., Baesens, B., Seow, H.-V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research*, 247(1), 124-136. <https://doi.org/10.1016/j.ejor.2015.05.030>
- [45]. Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes*, 151, 90-103. <https://doi.org/10.1016/j.obhdp.2018.12.005>
- [46]. Mashrur, A., Luo, W., Zaidi, N. A., & Robles-Kelly, A. (2020). Machine learning for financial risk management: A survey. *IEEE Access*, 8, 203203-203223. <https://doi.org/10.1109/access.2020.3036322>
- [47]. Md Anisur Rahman, M. (2024). State Income Tax Differentials and High-Skilled Labor Mobility in The United States: A Time Series Analysis. *American Journal of Interdisciplinary Studies*, 5(04), 222-267. <https://doi.org/10.63125/295bsn47>

- [48]. Md Anisur Rahman, M. (2025). The Role of AI-Enabled Business Intelligence in Financial Risk Assessment and Liquidity Monitoring. *Review of Applied Science and Technology*, 4(04), 195–246. <https://doi.org/10.63125/p4eezd93>
- [49]. Md Anisur Rahman, M. (2026). AI-Driven Business Intelligence for Real-Time Fraud Risk Monitoring in Digital Payment Platforms: A Framework-Based Review. *International Journal of Scientific Interdisciplinary Research*, 7(1), 527–580. <https://doi.org/10.63125/0ef34271>
- [50]. Md Arif Uz, Z., Sharmin, S., & Md Abdur, R. (2025). Factors Influencing Behavioural Intention to Use the Innovative Open And Distance Learning Systems With The Role Of Continuance Intention. *American Journal of Scholarly Research and Innovation*, 4(01), 202–220. <https://doi.org/10.63125/pbjxp014>
- [51]. Md Ashfaq, S., & Abdullah Mohammad, S. (2022). CNT/PANI Composite Electrodes for Flexible Fiber-Shaped Dye-Sensitized Solar Cells: Synthesis, Characterization, and Photovoltaic Performance. *American Journal of Interdisciplinary Studies*, 3(02), 221–274. <https://doi.org/10.63125/m334mf41>
- [52]. Md Asif Ali Sheak, A. (2024). A Meta-Analysis of Agile and Lean Project Management Methodologies in Large-Scale Engineering and IT Integration Projects. *American Journal of Data Science and Analytics*, 5(12), 202–240. <https://doi.org/10.63125/6281tn40>
- [53]. Md Asif Ali Sheak, A., & Risha, A. (2022). The Role of IOT-Driven Energy Analytics in Improving Operational Efficiency and Sustainability in Modern Industrial Facilities. *American Journal of Interdisciplinary Studies*, 3(04), 807–841. <https://doi.org/10.63125/gm63q956>
- [54]. Md Mahamud Pervaz, P. (2025). Development of a CMMS-Integrated Predictive Maintenance Framework for Industrial PLC and Drive Systems. *American Journal of Scholarly Research and Innovation*, 4(01), 894–942. <https://doi.org/10.63125/j33gtf31>
- [55]. Md Mahamud Pervaz, P. (2026). Implementation of an OSHA-Compliant Lockout/Tagout and Arc-Flash Hazard Mitigation Framework for U.S. Industrial Maintenance Operations. *American Journal of Interdisciplinary Studies*, 7(02), 73–119. <https://doi.org/10.63125/8ky04n07>
- [56]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, 1(4), 70–102. <https://doi.org/10.63125/dyrpc387>
- [57]. Mhlanga, D. (2021). Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. *International Journal of Financial Studies*, 9(3), 39. <https://doi.org/10.3390/ijfs9030039>
- [58]. Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management*, 58(3), 103434. <https://doi.org/10.1016/j.im.2021.103434>
- [59]. Milkau, U. (2021). Operational resilience as a new concept and extension of operational risk management. *Journal of Risk Management in Financial Institutions*, 14(4), 408–425. <https://doi.org/10.69554/qulw1579>
- [60]. Mohammad Abir Chowdhury, S. (2023). Role of AI-Assisted Risk Assessment in Enhancing Audit Planning Efficiency and Risk Prioritization in Public-Safety Organizations. *International Journal of Scientific Interdisciplinary Research*, 4(4), 529–576. <https://doi.org/10.63125/qd6nn437>
- [61]. Mohammad Abir Chowdhury, S. (2025). Application of Machine Learning and Anomaly-Detection Algorithms for Fraud Detection in U.S. Government Financial Operations. *American Journal of Interdisciplinary Studies*, 6(02), 139–184. <https://doi.org/10.63125/fkf19309>
- [62]. Mohammad Abir Chowdhury, S. (2026). Development Of a Machine-Learning Approach for Internal-Control Weakness Prediction and Audit-Risk Scoring In U.S. State Government Agencies. *American Journal of Data Science and Analytics*, 7(06), 380–424. <https://doi.org/10.63125/3v722074>
- [63]. Mohammad Abir Chowdhury, S., & Tonay, P. (2022). An Empirical Analysis of the Impact of Robotic Process Automation and Continuous Auditing on the Timeliness And Accuracy Of Financial Reporting Assurance. *International Journal of Business and Economics Insights*, 2(4), 73–126. <https://doi.org/10.63125/7p8dcr47>
- [64]. Mohammad Badrul, A. (2025). SCADA And IOT-Enabled Smart Water Metering: A Systematic Review of Resilient Supply Monitoring. *International Journal of Scientific Interdisciplinary Research*, 6(1), 576–615. <https://doi.org/10.63125/at8pnx81>
- [65]. Mohammad Badrul, A. (2026). A Machine-Learning Framework for Real-Time Non-Revenue Water Prediction in Aging Urban Distribution Networks. *American Journal of Interdisciplinary Studies*, 7(02), 01–52. <https://doi.org/10.63125/93km2h66>
- [66]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning-Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, 3(02), 33–77. <https://doi.org/10.63125/y3yfxa92>
- [67]. Muhammad Zahidul, I. (2023). Comparative Analysis of Machine-Learning Approaches for Pharmaceutical Sales Forecasting and Market-Demand Prediction. *Review of Applied Science and Technology*, 2(02), 38–95. <https://doi.org/10.63125/etcbqf13>
- [68]. Naiseh, M., Cemiloglu, D., Al-Thani, D., Jiang, N., & Ali, R. (2021). Explainable recommendations and calibrated trust: Two systematic user errors. *Computer*, 54(10), 28–37. <https://doi.org/10.1109/mc.2021.3076131>
- [69]. Nallakaruppan, M. K., Balusamy, B., Shri, M. L., Malathi, V., & Bhattacharyya, S. (2024). An explainable AI framework for credit evaluation and analysis. *Applied Soft Computing*, 153, 111307. <https://doi.org/10.1016/j.asoc.2024.111307>

- [70]. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559-569. <https://doi.org/10.1016/j.dss.2010.08.006>
- [71]. Nishat, J. (2025). Leveraging Machine Learning to Identify and Address Maternal Health Disparities in Underserved U.S. Communities. *American Journal of Data Science and Analytics*, 6(12), 125-169. <https://doi.org/10.63125/c2t7r719>
- [72]. Nishat, J. (2026). Predictive Analytics for Program Effectiveness: A Machine Learning Approach to Health Education Programs in the United States. *American Journal of Health and Medical Sciences*, 7(03), 30-56. <https://doi.org/10.63125/2vw42878>
- [73]. Nishat, J., & Jahanara, A. (2024). Machine Learning Approaches for Early Prediction of High-Risk Pregnancy in Underserved U.S. Populations. *American Journal of Interdisciplinary Studies*, 5(04), 268-309. <https://doi.org/10.63125/5gh5df13>
- [74]. Nishat, J., & Mst Kaniz, F. (2022). A Review of the Impact of Covid-19 On Maternal and Child Health Service Utilization in Bangladesh. *American Journal of Scholarly Research and Innovation*, 1(02), 223-269. <https://doi.org/10.63125/vgv5s742>
- [75]. Nuzhat Sadia, P. (2025). Integrating Business Intelligence Dashboards for Real-Time Supply Chain Visibility and Operational Decision Support. *American Journal of Data Science and Analytics*, 6(12), 170-216. <https://doi.org/10.63125/1es4f763>
- [76]. Nuzhat Sadia, P. (2026). An Integrated IT Management Framework for Scenario-Based Enterprise Analytics and Strategic Decision Optimization. *American Journal of Interdisciplinary Studies*, 7(02), 120-168. <https://doi.org/10.63125/3wtc3z49>
- [77]. Pavlou, P. A., & El Sawy, O. A. (2011). Understanding the elusive black box of dynamic capabilities. *Decision Sciences*, 42(1), 239-273. <https://doi.org/10.1111/j.1540-5915.2010.00287.x>
- [78]. Puranam, P. (2021). Human-AI collaborative decision-making as an organization design problem. *Journal of Organization Design*, 10, 75-80. <https://doi.org/10.1007/s41469-021-00095-2>
- [79]. Quah, J. T. S., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert Systems with Applications*, 35(4), 1721-1732. <https://doi.org/10.1016/j.eswa.2007.08.093>
- [80]. Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation-augmentation paradox. *Academy of Management Review*, 46(1), 192-210. <https://doi.org/10.5465/amr.2018.0072>
- [81]. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*,
- [82]. Ratzan, J., & Rahman, N. (2024). Measuring responsible artificial intelligence (RAI) in banking: A valid and reliable instrument. *AI and Ethics*, 4(4), 1279-1297. <https://doi.org/10.1007/s43681-023-00321-5>
- [83]. Rony, S., & Md, A. (2026). Multi-Agency Coordination in Sustained Healthcare Supply Shortages: Lessons from Covid-19, Drug Shortages, and Critical Medical Supply Disruptions. *American Journal of Data Science and Analytics*, 7(01), 181-221. <https://doi.org/10.63125/5v6t8515>
- [84]. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206-215. <https://doi.org/10.1038/s42256-019-0048-x>
- [85]. Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, 76, 130-157. <https://doi.org/10.1016/j.engappai.2018.07.008>
- [86]. Sachan, S., Almaghrabi, F., Yang, J.-B., & Xu, D.-L. (2024). Human-AI collaboration to mitigate decision noise in financial underwriting: A study on FinTech innovation in a lending firm. *International Review of Financial Analysis*, 93, 103149. <https://doi.org/10.1016/j.irfa.2024.103149>
- [87]. Saputra, M. P. A., Sukono, & Chaerani, D. (2022). Estimation of maximum potential losses for digital banking transaction risks using the extreme value-at-risks method. *Risks*, 10(1), 10. <https://doi.org/10.3390/risks10010010>
- [88]. Seeber, I., Bittner, E., Briggs, R. O., de Vreede, T., de Vreede, G.-J., Elkins, A., Maier, R., Merz, A. B., Oeste-Reiß, S., Randrup, N., Schwabe, G., & Söllner, M. (2020). Machines as teammates: A research agenda on AI in team collaboration. *Information & Management*, 57(2), 103174. <https://doi.org/10.1016/j.im.2019.05.004>
- [89]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, 3(04), 1-31. <https://doi.org/10.63125/negjw373>
- [90]. Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review*, 61(4), 66-83. <https://doi.org/10.1177/0008125619862257>
- [91]. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in FinTech applications. *Sensors*, 21(5), 1594. <https://doi.org/10.3390/s21051594>
- [92]. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319-1350. <https://doi.org/10.1002/smj.640>
- [93]. Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation*, 41, 100833. <https://doi.org/10.1016/j.jfi.2019.100833>
- [94]. Tonay, P. (2025). Machine Learning for Fraud Detection in Enterprise Financial Systems. *American Journal of Advanced Technology and Engineering Solutions*, 1(02), 304-318. <https://doi.org/10.63125/d0fhfp873>

- [95]. Tonay, P. (2026). The Role of AI-Based Decision Support in Financial Risk Management and Anomaly Detection. *American Journal of Data Science and Analytics*, 7(06), 327-359. <https://doi.org/10.63125/wnb54w77>
- [96]. Tonay, P., Md Maruf, I., & Al, A. (2024). Artificial Intelligence-Based Decision Support Systems and Managerial Performance. *American Journal of Advanced Technology and Engineering Solutions*, 4(04), 154-184. <https://doi.org/10.63125/wmz8dc67>
- [97]. Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research*, 70, 356-365. <https://doi.org/10.1016/j.jbusres.2016.08.009>
- [98]. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47-66. <https://doi.org/10.1016/j.cose.2015.09.005>
- [99]. Westphal, M., Vössing, M., Satzger, G., Yom-Tov, G. B., & Rafaeli, A. (2023). Decision control and explanations in human-AI collaboration: Improving user perceptions and compliance. *Computers in Human Behavior*, 144, 107714. <https://doi.org/10.1016/j.chb.2023.107714>
- [100]. Zhang, T., Zhang, W., Xu, W., & Hao, H. (2018). Multiple instance learning for credit risk assessment with transaction data. *Knowledge-Based Systems*, 161, 65-77. <https://doi.org/10.1016/j.knosys.2018.07.030>