World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

PREDICTIVE ANALYTICS FOR SUPPLIER RISK ASSESSMENT AND COST OPTIMIZATION IN FINANCIAL INSTITUTIONS

Alimatou Jallow [1], Mary Jatta [1], Sarah Cobbinah[1], Cynthia Ifebi [2], Sulyman Babatunde [3] and Yunus Ibrahim [4, *]

[1] School of Business, San Francisco Bay University, California, USA.
[2] Institute for Digital Technologies, Loughborough, University London, UK.
[3] The Fuqua School of Business, Duke University, North Carolina, USA.
[4] Darden School of Business, University of Virginia, Charlottesville, Virginia, USA.
* Corresponding Author

World Journal of Advanced Research and Reviews, 2026, 32(02), 1173–1182

Publication history: Received on 02 October 2026; revised on 08 November 2026; accepted on 10 November 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.32.2.2757

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Financial institutions now depend on a wide network of technology vendors, data providers, cloud platforms and service firms to deliver core functions. This dependence has moved supplier risk from a procurement concern to a prudential and resilience issue, while the cost of managing suppliers continues to grow. Predictive analytics offers a way to anticipate supplier failure, service disruption, cyber compromise and compliance breaches, and to link those forecasts to sourcing and contracting decisions. This article reviews the literature on predictive analytics for supplier risk assessment and cost optimization in financial institutions. It proposes a conceptual framework that connects supplier risk domains, predictive methods and management decisions, and it compares statistical, machine learning, deep learning, text-based and network-based techniques. Applications to financial-health scoring, cyber and operational risk, compliance screening and early-warning systems are examined, followed by applications to supplier selection, contract pricing, spend analytics and risk-adjusted cost modeling. Implementation issues covering data quality, model governance and explainability are discussed in light of current supervisory expectations. The literature appears concentrated on financial-distress prediction, whereas cyber, concentration and fourth-party risk, and the integration of risk forecasts into cost decisions, remain comparatively underdeveloped. Research gaps and future directions are proposed, including generative artificial intelligence, federated learning and shared industry data.

Keywords: Predictive Analytics; Supplier Risk; Third-Party Risk Management; Cost Optimization; Financial Institutions; Machine Learning; Operational Resilience

1 INTRODUCTION

Banks, insurers, asset managers and payment firms have steadily expanded the range of activities they obtain from external parties. Outsourcing began as a way to reduce cost in back-office functions, but it now extends to core banking platforms, payment processing, data storage, analytics, customer communication and cybersecurity operations [1]. The rise of cloud computing and of partnerships with financial technology firms has deepened this reliance and has made many institutions dependent on a small number of large service providers [2].

Dependence of this kind exposes an institution to the weaknesses of its suppliers. A supplier may become financially distressed, fail to deliver a service, suffer a cyber incident, breach a regulation or be affected by a geopolitical event. Well-publicized service outages and data breaches at third parties have shown how a single incident can spread across many institutions at once [3].

Since responsibility for an outsourced activity remains with the institution, supervisors have set detailed expectations for the management of third-party relationships, including interagency guidance in the United States that covers the full life cycle of such relationships [4]. Institutions are expected to assess supplier risk before engagement, monitor it throughout the relationship and plan for exit. Meeting these expectations requires due-diligence processes, contract reviews, audits and monitoring capacity for large numbers of suppliers.

Assessment based on periodic questionnaires, manual reviews and static risk tiers is, by design, slow to reflect change and tends to allocate effort evenly rather than where risk is greatest. Predictive analytics, which uses historical and current data to estimate the likelihood of future events, offers a more forward-looking and scalable alternative. It also creates an opportunity to connect risk and cost, because forecasts of supplier failure or disruption can be converted into expected losses and used to choose suppliers, negotiate contracts and allocate monitoring resources.

This review examines how predictive analytics has been applied to supplier risk assessment and to cost optimization in financial institutions. It addresses three questions. First, which predictive techniques have been used, and what are their strengths and limitations in this setting? Second, how have these techniques been applied to different supplier risk domains and to cost-related decisions? Third, what data, governance and methodological gaps limit adoption and what research directions could close them?

The remainder of the article is organized as follows. Section 2 presents the conceptual framework used to organize the literature, and Section 3 provides background and regulatory context. Section 4 reviews predictive techniques. Sections 5 and 6 examine applications to risk assessment and to cost optimization, respectively. Section 7 discusses data, implementation and governance. Sections 8 and 9 present challenges, research gaps and future directions, and Section 10 concludes.

2 CONCEPTUAL FRAMEWORK

The review considers peer-reviewed research, supervisory publications and industry standards that address the prediction of supplier-related risk or the use of such predictions in cost decisions. The term supplier is used broadly to cover vendors of technology and data services, outsourced service providers, cloud and infrastructure providers and other third parties on which an institution relies. Studies from manufacturing and retail supply chains are included where their methods transfer to financial services. Research on the credit risk of an institution's own borrowers is outside the scope, except where the same models are applied to the financial health of suppliers.

Emphasis is placed on work from the last decade. During this period, machine learning, text analytics and network methods matured, and supervisory attention to third-party risk increased, as discussed in Sections 3 and 4. Because the field is spread across operations research, finance, information systems and risk management, no single terminology is used, and the literature is therefore grouped by problem and method rather than by discipline.

The framework used to organize the review is shown in Figure 1. The left-hand side lists five supplier risk domains: financial health, operational continuity, cyber and information security, regulatory and compliance risk, and concentration and geopolitical risk. These domains follow the classification commonly used in the supplier risk literature [5]. The central layer represents the predictive analytics process, from data integration to the production of risk scores and early-warning signals, and it follows the development, validation and monitoring cycle expected under model risk management guidance [6]. The right-hand side lists the management decisions that these outputs inform, from supplier selection to contingency planning, which correspond to the stages of the third-party relationship life cycle described in Section 3.2. The final outcome is a lower risk-adjusted total cost of supplier relationships together with improved resilience. Sections 4 to 7 follow this logic, moving from methods to risk applications, cost applications and implementation.

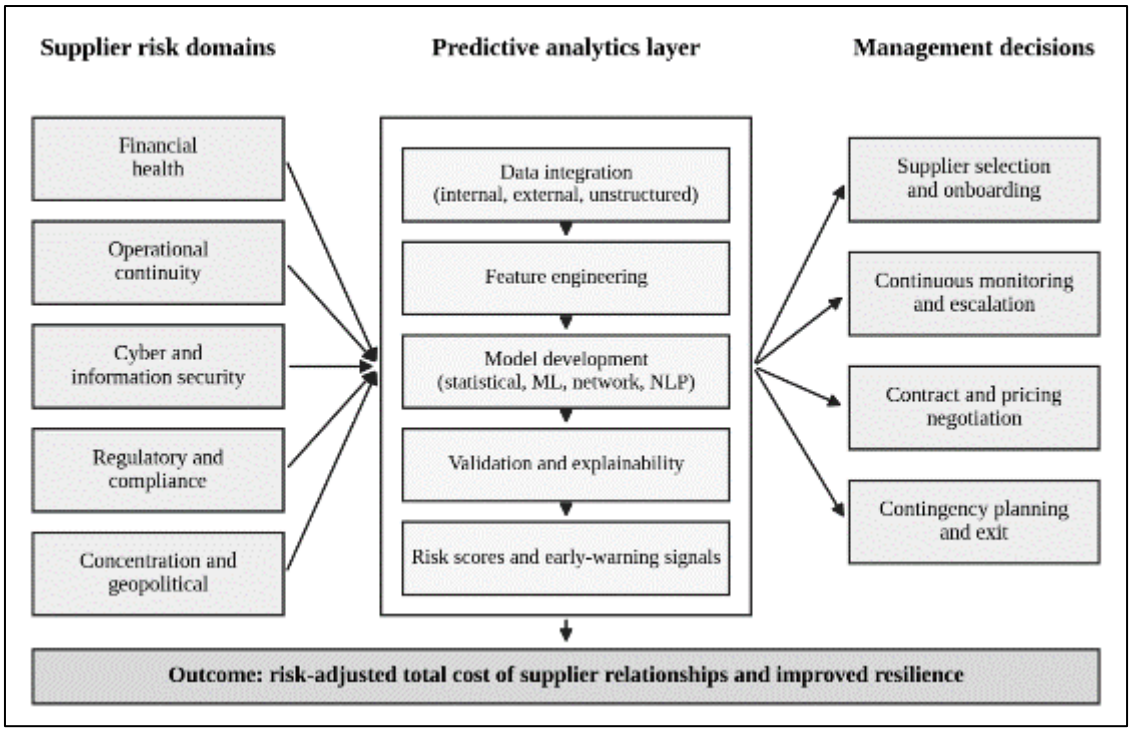


Figure 1: Conceptual framework linking supplier risk domains, the predictive analytics process and management decisions.

3 BACKGROUND AND REGULATORY CONTEXT

3.1 Supplier risk in financial institutions

Supplier risk is the possibility that a third party will fail to perform, or will behave in a way that harms the institution, its customers or its regulatory standing. It is commonly divided into financial, operational, cyber, compliance and strategic or concentration components, as outlined in Section 2. The categories overlap. A financially weak supplier may cut investment in security, and a cyber incident may cause both operational disruption and a compliance breach. Predictive models therefore need to capture correlated risks rather than treat each domain in isolation.

Concentration deserves particular attention in financial services. When many institutions rely on the same cloud or software provider, a single failure can affect a large part of the sector at the same time, so that supplier risk becomes a source of systemic risk [7]. Risk also travels through fourth parties, meaning the subcontractors of a supplier, which the institution does not contract with directly and often cannot observe [8]. Measuring exposure to these hidden dependencies is one of the main analytical challenges in the field.

3.2 Regulatory context

Regulation shapes both the demand for predictive tools and the limits on their use. The United States interagency guidance introduced in Section 1 describes planning, due diligence, contract negotiation, ongoing monitoring and termination as stages of a relationship life cycle, and it calls for oversight proportionate to the criticality of the activity. The European Banking Authority guidelines require a register of outsourcing arrangements and a risk assessment that considers concentration and substitutability [9]. The Digital Operational Resilience Act extends these ideas by setting requirements for the management of information and communication technology third-party risk and by creating oversight of critical providers. The Basel principles place third-party dependencies within the wider goal of operational resilience[10,11].

These frameworks do not prescribe particular analytical methods, but they create a demand for evidence-based, continuous and proportionate monitoring, which predictive models can supply. At the same time, model use is itself supervised. The model risk management guidance noted in Section 2 expects institutions to document models, validate them independently and monitor their performance. Any predictive system for supplier risk must therefore be built with governance in mind from the outset.

3.3 Cost structure of supplier management

The cost of a supplier relationship extends well beyond the contract price. Total cost of ownership includes the cost of searching for and selecting the supplier, due diligence, integration, monitoring, audit, remediation, and the expected cost of failure and exit [12]. Much of this cost is driven by risk. A supplier classed as high risk attracts more frequent reviews, more detailed controls and more contingency planning. If risk classification is inaccurate, effort is misallocated, with resources spent on low-risk suppliers while genuine threats are overlooked.

This link suggests two routes by which predictive analytics can reduce cost. The first is efficiency, by directing due diligence and monitoring toward the suppliers and events that matter most. The second is loss avoidance, by anticipating failures early enough to switch providers, renegotiate terms or activate contingency arrangements. Both routes depend on risk estimates that are accurate, timely and interpretable enough to support decisions.

4 PREDICTIVE ANALYTICS TECHNIQUES

The techniques reported in the literature can be grouped into six families, summarized in Figure 2. Their typical inputs, strengths and limitations are compared in Table 1.

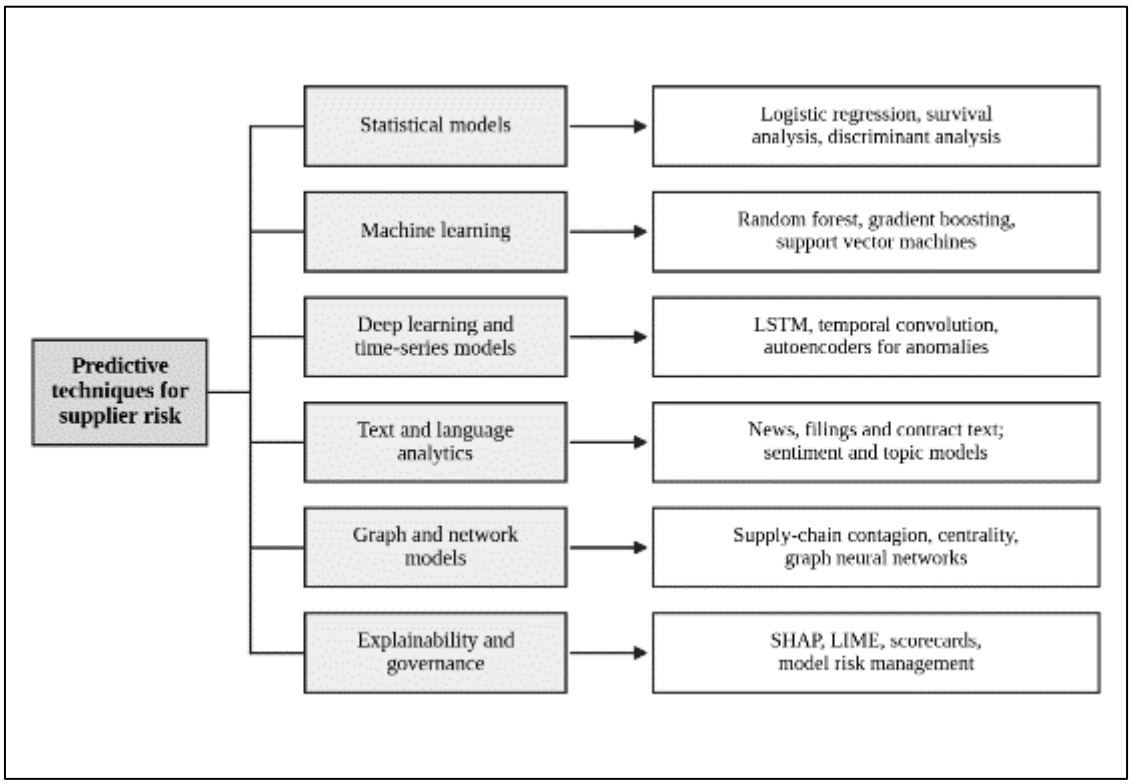


Figure 2: Taxonomy of predictive analytics techniques used for supplier risk assessment.

4.1 Statistical models

Logistic regression and discriminant analysis remain the reference methods for predicting failure from financial ratios, and they underlie many established scoring systems [13]. Their transparency, stability and ease of validation make them attractive to supervisors and risk committees. Survival and hazard models extend this approach by modeling the time until an event such as default or contract termination and by accommodating censored observations, which are common when many suppliers have not yet failed [14]. Their weakness is limited flexibility. They struggle with non-linear relationships and interactions among many variables, and they depend on carefully chosen predictors.

4.2 Machine learning

Tree-based ensembles are the most widely used machine learning methods for tabular risk data. Random forests average many decision trees grown on resampled data and are robust to noise and to irrelevant variables [15]. Gradient boosting builds trees sequentially so that each corrects the errors of its predecessors, and it often achieves the highest accuracy on structured data [16]. Comparative studies of bankruptcy and credit prediction generally report that machine learning methods, including support vector machines, outperform classical statistical models in discrimination, although the margin varies with the data set and the evaluation design [17].

Two cautions apply. First, supplier failure is a rare event, so data sets are highly imbalanced, and accuracy is a misleading metric. Studies that report precision, recall and precision-recall curves, or that use cost-sensitive evaluation, give a more realistic picture of usefulness [18]. Second, small differences in discrimination may not justify the loss of transparency, especially where the model informs a supervised process. The choice of technique should therefore reflect the decision context and not accuracy alone.

4.3 Deep learning and time-series models

Recurrent and convolutional networks can learn from sequences of observations, such as monthly payment behavior, service-level metrics or incident counts. Long short-term memory networks are the most common architecture for this purpose and can capture temporal patterns that static models miss [19]. Autoencoders and related unsupervised methods are used to detect anomalies, for example unusual changes in a supplier's transaction pattern, in settings where labeled failures are scarce [20]. Deep models generally need larger data sets than most institutions hold on their own suppliers, and their opacity raises validation difficulties. Evidence of a consistent advantage over boosted trees on tabular supplier data remains limited.

4.4 Text and network analytics

A large share of the information relevant to supplier risk is unstructured. Natural language processing can extract signals from annual reports, regulatory filings, contracts, audit reports and news. Transformer-based language models tuned to financial text have improved the classification of sentiment and risk-related disclosures [21]. Studies using news and social media suggest that sentiment and event detection can provide early evidence of deterioration before it appears in financial statements [22].

Network methods address the problem of interdependence. Representing suppliers, subcontractors and institutions as a graph makes it possible to measure exposure through indirect links and to simulate how a failure propagates through the network [23]. Graph neural networks learn from both the attributes of each node and the structure of its connections, and they have been proposed for detecting risky entities in relational data [24]. The main obstacle is data. Complete maps of supplier relationships, particularly at the fourth-party level, are rarely available.

4.5 Explainability

Explainability techniques allow complex models to be used where transparency is required. Shapley-value methods attribute a prediction to individual features and give both local and global explanations [25]. Local surrogate methods approximate the behavior of a complex model near a single prediction. These tools help analysts understand why a supplier was flagged and support challenge by risk committees and validators. They do not remove the need for sound model design, however, because explanations can be unstable when predictors are correlated.

Table 1: Comparison of predictive technique families for supplier risk assessment.

Technique family	Typical data	Strengths	Limitations
Statistical models (logistic, survival)	Financial ratios, payment history	Transparent, stable, easy to validate and explain to supervisors	Limited handling of non-linearity and interactions; predictor selection is manual
Tree ensembles (random forest, boosting)	Mixed structured data	High discrimination on tabular data; handles missing values and interactions	Less transparent; sensitive to class imbalance and to data drift
Deep learning and time-series	Sequences of behavioral and operational metrics	Captures temporal patterns; useful for anomaly detection	Data-hungry; opaque; limited evidence of advantage on tabular data
Text and language analytics	News, filings, contracts, reports	Adds early and unstructured signals; broad coverage	Noisy sources; language and domain shift; verification burden
Graph and network models	Supplier and fourth-party relationships	Reveals indirect exposure and concentration; supports contagion simulation	Relationship data are incomplete; hard to validate
Explainability tools	Outputs of any model	Supports challenge, audit and regulatory acceptance	Explanations may be unstable; add to, but do not replace, sound design

5 APPLICATIONS TO SUPPLIER RISK ASSESSMENT

Applications of predictive analytics to supplier risk differ by risk domain in the outcome being predicted, the data available and the methods that are usually applied. Table 2 summarizes these differences, and the sections that follow discuss each domain in turn.

Table 2: Predictive targets, data and methods by supplier risk domain.

Risk domain	Predictive target	Typical data	Common methods
Financial health	Probability of default or insolvency within a set horizon	Financial ratios, payment behavior, credit data	Logistic regression, survival models, boosted trees
Operational continuity	Service outage or missed obligation	Service-level metrics, incident and ticket histories	Time-series models, anomaly detection
Cyber and information security	Likelihood of a breach or security incident	External security ratings, breach history, access telemetry	Supervised classifiers, security scoring
Compliance and ESG	Sanctions, misconduct or disclosure risk	News, watch lists, disclosures, contracts	Text classification, language models
Concentration and fourth-party	Shared dependency and contagion exposure	Relationship maps, contract registers	Network analysis, graph models, simulation

5.1 Financial health and distress prediction

Financial-distress prediction is the most mature application. Models use balance-sheet and income ratios, market data, payment behavior and credit-bureau information to estimate the probability that a supplier will default or become insolvent within a set horizon [26]. For financial institutions the practical value lies in identifying critical suppliers whose failure would interrupt an important service. Many suppliers, especially technology start-ups and private firms, publish limited financial data, so models often combine sparse statements with alternative signals such as payment delays, staff turnover, funding events and web presence.

5.2 Cyber and operational risk

Cyber risk prediction for suppliers draws on external indicators such as exposed services, patching behavior, certificate hygiene and breach history, which are aggregated into security ratings, together with internal telemetry on the connections the supplier has to the institution [27]. Supervised models have been used to estimate the likelihood of a breach or incident, although the small number of labeled events and the changing nature of threats limit reliability. The relationship between external ratings and actual incidents is still debated, and ratings are best treated as one input among several.

Operational risk prediction focuses on service continuity. Models use service-level performance, incident and ticket histories, delivery delays and change events to forecast outages or missed obligations [28]. Time-series and anomaly-detection methods are common in this area, since deterioration in performance often precedes a serious failure. The main challenge is that institutions observe only the parts of a supplier's operation that touch their own services.

5.3 Compliance and ESG risk

Compliance risk includes exposure to sanctions, corruption, data-protection breaches and labor or environmental violations by suppliers. Text mining of adverse media, screening against watch lists and the classification of environmental, social and governance disclosures are typical applications [29]. These tasks are well suited to language models, but they also have high false-positive rates, so the amount of manual review can offset the efficiency gain. Studies that measure the reduction in analyst workload for a given level of detection are few.

5.4 Early-warning systems

Early-warning systems combine signals from several domains into a single monitored score or set of alerts. Reported designs use thresholds on model outputs, changes in score over time, or ensembles that weight financial, operational and cyber indicators [30]. The value of such systems depends on the lead time they provide and on the balance between missed events and false alarms. An alert that arrives too late or too often is not useful. Few studies evaluate lead time or alert workload in a live supplier-management setting, which limits the evidence on real-world benefit.

6 APPLICATIONS TO COST OPTIMIZATION

6.1 Supplier selection and portfolio design

Supplier selection has long been treated as a multi-criteria decision that balances price, quality, delivery and risk. Data-driven approaches replace subjective weights with predicted performance and failure probabilities, and they combine these with optimization models to choose among candidates [31]. In financial institutions, selection is also a portfolio problem, since the aim is to avoid excessive concentration in one provider or in providers that share common dependencies. Optimization models that impose limits on concentration or on the joint failure probability of critical services follow directly from this view.

6.2 Contract and pricing optimization

Predictive models can inform the terms of contracts as well as the choice of counterparty. Estimates of the cost and probability of disruption can be used to set service-level targets, penalties, insurance requirements and step-in rights, and to judge whether a lower price justifies a higher risk [32]. Analytics based on historical price and volume data can also identify contracts priced above benchmarks or renewals that offer scope for renegotiation [33]. The literature on this topic is dominated by applications in manufacturing and public procurement, and applications specific to financial institutions are scarce.

6.3 Spend analytics

Spend analytics classifies and consolidates expenditure across business units to reveal duplicated suppliers, maverick spending and opportunities for consolidation. Machine learning is used to categorize transactions, match supplier names and forecast demand [34]. For financial institutions, spend analytics also supports risk management, since a consolidated view of who is paid and for what is the starting point for a complete supplier inventory. Data quality is the main constraint, because supplier records are often duplicated or inconsistent across systems.

6.4 Risk-adjusted cost modeling

The clearest link between the two themes of this review is risk-adjusted cost modelling. Here the expected cost of supplier failure, derived from a predicted probability of failure and an estimate of loss, is added to the direct cost of the relationship. Stochastic and robust optimization models then choose suppliers, inventory or backup capacity to minimize this total under uncertainty [35]. Applications in the financial sector remain largely conceptual. Reliable loss estimates for service failure are difficult to obtain, and institutions rarely publish the cost data that would permit empirical testing.

7 DATA, IMPLEMENTATION AND GOVERNANCE

7.1 Data sources and quality

Effective models require data from internal and external sources. Internal sources include contract records, payment and invoice data, service-level reports, incident logs and audit findings. External sources include financial statements, credit and payment data, news, security ratings and regulatory databases. The main difficulties are fragmentation across systems, inconsistent supplier identifiers, missing data for private firms and the small number of recorded failures. Entity resolution and data linkage are therefore preconditions for modeling, and their cost is often underestimated in research studies.

7.2 Development and deployment pipeline

Figure 3 summarizes a typical pipeline. Data are collected and linked, features are constructed, models are trained and validated, and the resulting scores are deployed to the teams that manage suppliers. Because supplier risk changes over time and because regulatory and economic conditions shift, deployment is not the end of the process. Monitoring for drift and periodic recalibration are essential, and the validation step should include out-of-time testing, calibration checks and stress scenarios in addition to standard discrimination metrics [36].

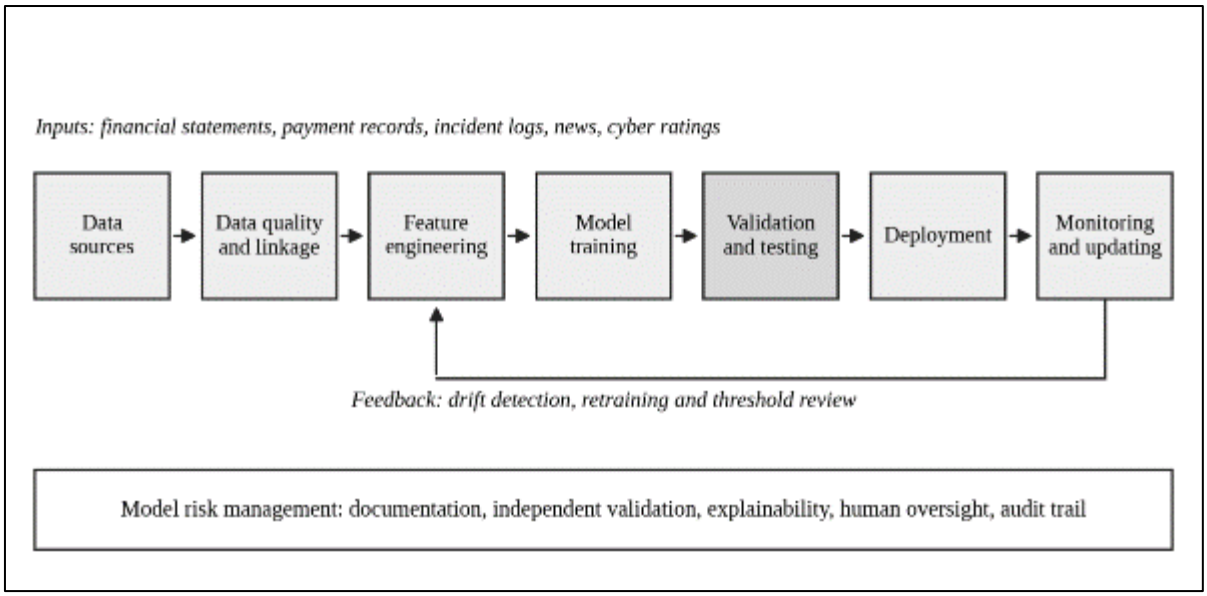


Figure 3: Development, deployment and monitoring pipeline for a supplier risk prediction system.

7.3 Model risk management and explainability

Predictive models used in supplier oversight fall within the model risk management expectations noted in Section 2. Institutions need documented purpose and assumptions, independent validation, ongoing performance monitoring and clear ownership. Human oversight is essential, since a model score should support and not replace the judgment of a risk professional. Explainability helps to meet these expectations, and the methods described in Section 4.5 can be used to show which factors drive a supplier's score. Institutions should also consider fairness and consistency, for example whether small or new suppliers are disadvantaged by limited data rather than by real risk.

8 CHALLENGES AND RESEARCH GAPS

Several challenges emerge from the literature. The first is data scarcity. Failures of critical suppliers are rare, labeled data are limited, and institutions hold information only on their own suppliers. As a result, models are often trained on proxy outcomes such as credit ratings or incidents that only partly reflect the risk of interest. The second is the gap between prediction and decision. Most studies report classification performance and stop, without showing how the predictions change sourcing, contracting or monitoring decisions, or what savings result.

The third challenge concerns interdependence. Fourth-party and concentration risks are recognized by supervisors but are seldom modeled empirically, because the required relationship data are missing. The fourth is validation and reproducibility. Studies frequently use different data sets, horizons and metrics, and few use out-of-time evaluation or report calibration, so results are hard to compare [37]. The fifth is the balance between accuracy and interpretability under regulatory scrutiny, which limits the adoption of complex models. Finally, evidence from operational settings is thin. Very few studies report results from live deployment in a financial institution, in part because of confidentiality.

9 FUTURE DIRECTIONS

Large language models and other generative methods are likely to change how unstructured supplier information is processed. They can summarize due-diligence documents, extract obligations from contracts and support analysts in reviewing adverse news [38]. Their use in a regulated setting raises questions about reliability, hallucination, data confidentiality and auditability, and rigorous evaluation against human review is needed before they are relied upon.

Federated learning and privacy-preserving computation could address the data scarcity problem by allowing institutions to train shared models without pooling raw data [39]. Such approaches could support industry-level early-warning models for common suppliers and better estimates of concentration risk. Continuous monitoring based on real-time data feeds, richer relationship graphs that include fourth parties, and causal methods that go beyond prediction to estimate the effect of interventions are further directions. Finally, studies that quantify the financial benefit of predictive supplier risk management, using field evidence or credible simulation, would strengthen the case for adoption.

10 CONCLUSION

Supplier risk has become a central concern for financial institutions, driven by growing outsourcing, concentration in a small number of providers and demanding supervisory expectations. Predictive analytics provides tools to anticipate supplier failure, disruption, cyber compromise and compliance breaches, and to connect those forecasts to decisions on selection, contracting and monitoring. This review has organized the literature through a framework that links risk domains, predictive methods and management decisions.

The evidence suggests that mature techniques exist for financial-distress prediction and that machine learning, text analytics and network methods offer promising extensions. At the same time, the field is limited by scarce data, weak evaluation practices, a lack of empirical work on concentration and fourth-party risk, and little evidence linking predictions to realized cost savings. Progress will depend on integrating risk prediction with cost decisions, on better data sharing that respects confidentiality, and on models that satisfy supervisory demands for governance and explainability. Addressing these gaps would allow financial institutions to reduce the cost of supplier management while strengthening their operational resilience.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

[1] Allen F, Santomero AM. What do financial intermediaries do?. Journal of banking & finance. 2001 Feb 1;25(2):271-94.

[2] Adrian T. BigTech in financial services. International Monetary Review. 2021;8(3):90-4.

[3] Wolff J, Lehr W. Ex-Post Mitigation Strategies for Breaches of Non-Financial Data. TPRC.

[4] Pierides M, Mulligan J. Key themes of resiliency, outsourcing and third-party risk management regimes. Journal of Securities Operations & Custody. 2025 Jan 1;17(2):102-18.

[5] Chapelle A. Operational risk management: Best practices in the financial services industry. John Wiley & Sons; 2018 Dec 10.

[6] Omoruyi N. Advanced computational methods for financial planning and analysis risk assessment using data science-driven model validation techniques. International Journal of Research Publication and Reviews. doi: https://www. semanticscholar. org/paper/4d27d96c40e20c0bd7df2d9220bd4b355a381c82. 2025.

[7] Gozman D, Machaiah T, Willcocks L. Cloud sourcing and mitigating concentration risk in financial services. InInformation Systems Outsourcing: The Era of Digital Transformation 2020 Jun 5 (pp. 335-358). Cham: Springer International Publishing.

[8] Parella K. Protecting third parties in contracts. American Business Law Journal. 2021 Jul;58(2):327-86.

[9] Giani L, Vetrone A. The Broadening Scope of Financial Regulation: Digital Operational Resilience and Cloud Computing. University of Genoa Centre for Law and Finance–Research Working Paper. 2026 Dec 19(4).

[10] Peihani M. Regulation of cyber risk in the banking system: a Canadian case study. Journal of Financial Regulation. 2022 Sep;8(2):139-61.

[11] Bida A, Nathoo R. Operational resilience towards a global alignment. Journal of Business Continuity & Emergency Planning. 2024 Jan 1;17(4):306-22.

[12] Ellram LM. Total cost of ownership: an analysis approach for purchasing. International journal of physical distribution & logistics management. 1995 Oct 1;25(8):4-23.

[13] Altman EI. Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. The journal of finance. 1968 Sep 1;23(4):589-609.

[14] Gupta J, Gregoriou A, Ebrahimi T. Empirical comparison of hazard models in predicting SMEs failure. Quantitative Finance. 2018 Mar 4;18(3):437-66.

[15] Mohammadpour SI, Vahedi J. Improved Balanced Random Forest (iBRF): A flexible hybrid resampling-bagging framework for crash severity classification in imbalanced datasets. Traffic Injury Prevention. 2026 Jan 8:1-9.

[16] Mabrouke F, Al-Sahili B, Assaf R, Al-Sartawi A, Aljazzar S, Zahran S, Kanan M. Evaluating the performance of serial production lines using tree-based machine learning methods. Reports in Mechanical Engineering. 2025 Jun 24;6(1):27-45.

[17] Le HH, Viviani JL. Predicting bank failure: An improvement by implementing a machine-learning approach to classical financial ratios. Research in international business and finance. 2018 Apr 1;44:16-25.

[18] Baryannis G, Dani S, Antoniou G. Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. Future Generation Computer Systems. 2019 Dec 1;101:993-1004.

[19] Van Houdt G, Mosquera C, Nápoles G. A review on the long short-term memory model. Artificial intelligence review. 2020 Dec;53(8):5929-55.

[20] Vankayalapati RH, Banerjee A. A systematic review on applications of deep learning in supply chain risk management. InOperations Research Forum 2026 Aug 5 (Vol. 7, No. 3, p. 94). Cham: Springer International Publishing.

[21] Li Y, Jiang X, Wang Y. TRAM-FIN: A transformer-based real-time assessment model for financial risk detection in multinational corporate statements. Journal of Advanced Computing & Intelligent Systems. 2023 Sep 17;3(9):54-67.

[22] Hajek P, Munk M. Speech emotion recognition and text sentiment analysis for financial distress prediction. Neural Computing and Applications. 2023 Oct;35(29):21463-77.

[23] Kim Y, Chen YS, Linderman K. Supply network disruption and resilience: A network structural perspective. Journal of operations Management. 2015 Jan;33(1):43-59.

[24] Kim H, Lee BS, Shin WY, Lim S. Graph anomaly detection with graph neural networks: Current status and challenges. IEEe Access. 2022 Oct 3;10:111820-9.

[25] Li M, Sun H, Huang Y, Chen H. Shapley value: from cooperative game to explainable artificial intelligence. Autonomous Intelligent Systems. 2024 Feb 9;4(1):2.

[26] Hernandez Tinoco M. Financial distress and bankruptcy prediction using accounting, market and macroeconomic variables. University of Leeds; 2013.

[27] Hu K, Levi R, Yahalom R, Zerhouni EG. Supply chain characteristics as predictors of cyber risk: A machine-learning assessment. IEEE Transactions on Dependable and Secure Computing. 2025 May 19;22(5):5648-57.

[28] Prasetio S, Wibisono G. Design and Evaluation of Incident Forecasting Improvement With Deep Learning Toward a Predictive Maintenance Framework in the Contact Center Industry. IEEE Access. 2025 Nov 10;13:197257-76.

[29] Akinleye OK, Adeyoyin O. A Category Spend Mapping and Supplier Risk Assessment Framework for Global Supply Chains.

[30] Ullah N, Ishaq M, Rahman F, Aslam MU, Adil F. An Advanced AI-Driven Risk Assessment Framework for US Banking Institutions: Integrating Predictive Financial Analytics, Regulatory-Aware Governance and Cybersecurity Risk Intelligence. Journal of Management Science Research Review. 2026 Jun 30;5(2):3176-204.

[31] Wang Y, Wang J, Zhang H, Song J. Bridging prediction and decision: Advances and challenges in data-driven optimization. Nexus. 2025 Mar 18;2(1).

[32] Samson D, Gloet M. Integrating performance and risk aspects of supply chain design processes. Production Planning & Control. 2018 Nov 18;29(15):1238-57.

[33] Kufile OT, Akinrinoye OV, Umezurike SA, Ejike OG, Otokiti BO, Onifade AY. Advances in data-driven decision-making for contract negotiation and supplier selection. International Journal of Multidisciplinary Research and Growth Evaluation. 2022 Mar;3(2):831-42.

[34] Agrawal N, Cohen MA, Deshpande R, Deshpande V. How machine learning will transform supply chain management. Harvard Business Review. 2024 Mar 1;103(3-4):128-37.

[35] Govindan K, Cheng TC. Advances in stochastic programming and robust optimization for supply chain planning. Computers & Operations Research. 2018 Dec 1;100:262-9.

[36] Quell P, Bellotti AG, Breeden JL, Martin JC. Machine learning and model risk management. Model Risk Manager's International Association.(mrmia. org). 2021.

[37] Voicila Voicila I, Urquia Grande E. Advances in Business Failure: A Review of Progress and Prediction Methods. Journal of Economic Surveys. 2026 Aug 3.

[38] Davenport MJ. Enhancing legal document analysis with large language models: a structured approach to accuracy, context preservation, and risk mitigation. Open Journal of Modern Linguistics. 2025 Apr;15(2):232-80.

[39] Hasan MT, Kudapa SP. Data privacy-aware machine learning and federated learning: A framework for data security. American Journal of Interdisciplinary Studies. 2021 Sep 24;2(03):01-34.