



Explainable Artificial Intelligence for Continuous Supplier Risk Assessment and Proactive Mitigation Across United States Supply Networks

Igbinabor Okunbor

Delta State University, Nigeria

DOI : <https://doi.org/10.55248/gengpi.07.0926.2920>

ABSTRACT :

United States supply networks increasingly depend on complex ecosystems of manufacturers, logistics providers, technology vendors, contractors, and specialized service organizations whose changing conditions can create substantial operational exposure. Traditional supplier assessments based on periodic scorecards, questionnaires, audits, and static risk indicators may provide limited visibility into rapidly evolving financial, operational, cybersecurity, and dependency-related vulnerabilities. This study develops an Explainable Artificial Intelligence (XAI) framework for continuous supplier risk assessment and proactive mitigation across United States supply networks. The framework integrates multi-source supplier data with temporal machine learning, anomaly detection, dependency analysis, and dynamic risk scoring to identify emerging deterioration before significant disruption occurs. Explainability mechanisms provide supplier-specific attribution of risk to underlying indicators, enabling procurement and risk teams to understand why risk classifications change and evaluate model-generated warnings. Predicted probability, deterioration persistence, operational criticality, substitutability, and network exposure are subsequently combined to prioritize intervention. The framework links risk intelligence with supplier engagement, inventory protection, alternative sourcing, enhanced monitoring, and contingency activation, establishing a transparent, continuously learning approach to predictive supplier resilience management.

Keywords: Explainable Artificial Intelligence; Supplier Risk Assessment; Supply Chain Resilience; Predictive Analytics; Third-Party Risk; Proactive Risk Mitigation

1. INTRODUCTION

1.1 Growing Complexity of Supplier Risk Across United States Supply Networks

United States supply networks increasingly depend on interconnected ecosystems of manufacturers, logistics providers, technology vendors, contractors, cloud-service providers, and specialized third parties [1]. Globalization has extended sourcing across jurisdictions, while outsourcing has transferred critical production, technology, and service capabilities beyond direct organizational control [2]. Digital integration further connects suppliers through enterprise platforms, APIs, cloud infrastructure, and shared information environments. Simultaneously, lean inventory strategies reduce buffers available to absorb unexpected supply interruptions [3]. Multi-tier sourcing adds another layer of complexity because direct suppliers may depend on upstream organizations that remain poorly visible to purchasing firms [4]. Consequently, disruption originating from a single supplier can propagate through shared materials, technologies, transportation routes, or production dependencies, ultimately affecting manufacturing schedules, distribution capacity, service availability, and customer fulfilment across interconnected supply networks [5].

1.2 Limitations of Periodic and Static Supplier Risk Assessment

Conventional supplier-risk assessment commonly relies on questionnaires, scorecards, scheduled audits, financial reviews, compliance assessments, and manually assigned risk classifications [3]. These mechanisms provide structured snapshots of supplier conditions but can lose relevance as circumstances change between assessment cycles. Financial deterioration, capacity constraints, cyber incidents, logistics disruption, or geopolitical developments may emerge considerably faster than periodic reviews can capture [6]. Static classifications can also obscure deterioration trajectories because they emphasize current status rather than the direction, persistence, and acceleration of changing indicators [7]. Consequently, organizations may continue relying on previously acceptable supplier ratings even when more recent operational or external evidence indicates increasing vulnerability and a growing probability of disruption.

1.3 Emergence of AI and Continuous Supplier Risk Intelligence

Artificial intelligence enables supplier assessment to shift from retrospective evaluation toward continuous and forward-looking risk intelligence [2]. Machine-learning models can integrate financial, operational, cybersecurity, logistics, commercial, and external information to identify patterns associated with emerging supplier deterioration. Temporal analytics capture rolling trends, persistence, volatility, and acceleration, while anomaly detection identifies behaviour that deviates materially from supplier-specific baselines [5]. As new observations become available, dynamic risk scores can be recalculated rather than remaining fixed until the next formal assessment [7]. This approach enables weak deterioration signals to be detected before they develop into significant supply interruption. However, increasing reliance on algorithmic predictions introduces a parallel requirement for explainability [8]. Procurement and resilience teams require transparent evidence showing which indicators influenced a supplier's changing risk classification before consequential sourcing, escalation, or continuity decisions are undertaken [9].

1.4 Aim, Scope, and Contribution

This article develops an Explainable Artificial Intelligence framework for continuous supplier risk assessment across United States supply networks. The framework integrates multi-domain supplier information within a temporally synchronized analytical environment to identify evolving deterioration and generate supplier-specific disruption predictions [1]. Explainable scoring identifies the factors driving changes in predicted exposure, while dependency analysis incorporates supplier criticality, network position, substitutability, and potential disruption propagation [5]. Predictive outputs are subsequently connected with proactive interventions including enhanced monitoring, supplier engagement, alternative sourcing, inventory protection, and continuity activation [8]. Human oversight provides validation and decision accountability before significant interventions occur. Finally, observed supplier outcomes are returned to the analytical process to support model recalibration, threshold refinement, and continuous learning [6].

2. CONCEPTUAL FOUNDATIONS OF EXPLAINABLE SUPPLIER RISK INTELLIGENCE

2.1 Evolution of Supplier Risk Management

Supplier risk management has evolved from localized qualification and performance monitoring toward enterprise-wide oversight of interconnected third-party relationships [7]. Earlier approaches concentrated primarily on price, quality, delivery reliability, contractual compliance, and supplier financial capacity. Outsourcing subsequently transferred greater portions of production, logistics, technology, and specialized services to external organizations, increasing dependence on supplier continuity [10]. Digital procurement has further connected suppliers through electronic sourcing platforms, APIs, cloud applications, and integrated enterprise systems [13]. At the same time, multi-tier relationships can obscure upstream dependencies because strategic suppliers frequently rely on manufacturers, technology providers, logistics networks, and infrastructure outside the buyer's direct visibility [8]. Consequently, supplier disruption may propagate across multiple facilities, products, and services rather than remain confined to one contractual relationship. Modern supplier management therefore increasingly requires enterprise-wide intelligence capable of representing interconnected exposure and potential cascading consequences [15].

2.2 Multidimensional Nature of Supplier Risk

Supplier vulnerability emerges from multiple risk domains whose effects can reinforce one another over time [9]. Financial risk includes liquidity deterioration, excessive leverage, declining profitability, or payment instability, whereas operational risk encompasses capacity constraints, downtime, workforce disruption, and production instability. Quality failures can increase rejection rates and interrupt production, while logistics risk includes transportation delays, port disruption, inventory shortages, and lead-time volatility [12]. Cybersecurity exposure arises from vulnerabilities, compromised credentials, ransomware, cloud dependency, and insecure digital connections. Compliance risk concerns regulatory or contractual violations, while geopolitical and environmental risks include conflict, trade restrictions, extreme events, and infrastructure disruption [16]. Commercial pressures such as abrupt price changes or contract renegotiation provide additional indicators. Importantly, these domains are not independent: financial stress may reduce cybersecurity investment or maintenance expenditure, subsequently contributing to operational deterioration and declining service performance [11].

2.3 From Static Risk Scores to Continuous Predictive Assessment

Supplier analytics can be distinguished according to whether they describe existing conditions, diagnose underlying causes, predict future disruption, or support proactive intervention [8]. Static scorecards primarily describe supplier status at a particular assessment point, whereas diagnostic analytics examine why performance has changed. Predictive models estimate the probability of subsequent deterioration, and proactive analytics connect those estimates with mitigation decisions [14]. This progression is important because supplier risk is inherently time-dependent. A temporary delivery exception may have little predictive significance, while repeated delays accompanied by deteriorating financial or quality indicators can represent an emerging trajectory [10]. Rolling observations capture recent behaviour, anomalies identify departures from supplier-specific baselines, and persistence distinguishes sustained deterioration from isolated variation [16]. Trend acceleration can provide additional early-warning information by identifying suppliers whose risk indicators are worsening at increasing rates before conventional thresholds are breached.

2.4 Explainable Artificial Intelligence in Supplier Decision-Making

Explainable Artificial Intelligence enables predictive performance to be accompanied by evidence describing how models generate supplier-risk estimates [7]. Global explainability identifies variables that influence predictions across the broader supplier population, whereas local explanations reveal why a particular supplier received a specific risk score or classification [13]. Interpretable models can provide transparent coefficients or decision structures, while post-hoc techniques can estimate feature contributions for more complex machine-learning models [15]. Risk attribution may therefore show whether an elevated prediction is primarily associated with financial deterioration, repeated delivery failures, cyber vulnerabilities, geopolitical exposure, or interacting indicators. Such transparency becomes particularly important when predictions influence commercially significant decisions [9]. Procurement teams require defensible explanations before increasing supplier scrutiny, restricting purchasing activity, qualifying alternatives, changing sourcing allocations, or reconsidering contractual relationships. Explainability also enables human reviewers to challenge predictions that conflict with credible contextual information.

2.5 Research Gap and Analytical Positioning

A significant analytical gap remains between conventional supplier monitoring and continuous, explainable predictive risk intelligence [11]. Existing processes frequently separate financial, operational, cyber, logistics, compliance, and external-risk information across different systems and organizational functions. Even where predictive models are employed, high-performing algorithms may provide insufficient supplier-specific explanation or remain disconnected from practical mitigation pathways [14]. The framework developed in this article addresses this gap by integrating heterogeneous supplier signals within a common temporal architecture, detecting evolving deterioration, generating dynamic supplier-specific predictions, and explaining the factors responsible for changing risk levels [16]. Dependency-aware prioritization and human validation subsequently connect predictive evidence with proportionate intervention and continuous organizational learning [12].

3. MULTI-SOURCE SUPPLIER DATA ARCHITECTURE AND TEMPORAL RISK ENGINEERING

3.1 Financial and Commercial Risk Data

Financial and commercial information provides early evidence of whether a supplier's capacity to sustain contractual obligations is deteriorating [15]. Relevant financial indicators include liquidity ratios, leverage, working-capital adequacy, profitability trends, operating cash flow, debt-servicing capacity, and changes in external credit assessments. Payment behaviour can reveal delayed settlements or increasing dependence on accelerated receivables, while declining cash generation may indicate emerging financial pressure [18]. Commercial signals complement formal accounting information by capturing abrupt pricing changes, contract amendments, minimum-order adjustments, purchasing patterns, and unusual order volatility [21]. Supplier requests for advance payment or repeated renegotiation of contractual terms may also indicate changing conditions. These observations become more informative when evaluated longitudinally rather than independently. Persistent deterioration across liquidity, cash flow, payment behaviour, and commercial terms can provide earlier warning than annual financial statements alone [24].

3.2 Operational, Quality, and Logistics Signals

Operational and logistics data reveal whether emerging supplier pressures are beginning to affect execution capability [16]. Indicators should include delivery delays, lead-time variability, capacity utilization, production output, equipment downtime, order-fulfilment ratios, and service-level performance. Quality information including defect rates, returns, rejected deliveries, corrective-action frequency, and repeated nonconformities can identify deterioration that may eventually constrain production continuity [19]. Logistics variables should capture shipment frequency, transportation delays, missed milestones, route disruption, and changes in expected arrival patterns [22]. These indicators should be interpreted jointly because isolated exceptions may represent normal operational variability. Repeated delivery slippage accompanied by falling output, rising defects, and increasing corrective actions provides stronger evidence of deterioration. Monitoring deviations from supplier-specific performance expectations therefore enables operational weaknesses to be identified before they develop into sustained downstream shortages or customer-fulfilment disruption [17].

3.3 Cybersecurity, Compliance, and External Risk Indicators

Supplier assessment should extend beyond internal performance because disruptions may originate from digital, regulatory, geopolitical, or environmental conditions [20]. Cybersecurity indicators can include reported incidents, unresolved vulnerabilities, ransomware activity, authentication anomalies, exposed services, and abnormal third-party access. Compliance intelligence should capture regulatory enforcement, certification failures, sanctions exposure, and material legal or policy changes [23]. External indicators should additionally incorporate geopolitical instability, extreme weather, commodity-price volatility, infrastructure interruption, regional economic deterioration, and transportation constraints. These signals can modify the significance of supplier-specific observations. For example, declining delivery reliability may warrant greater concern when facilities are simultaneously exposed to infrastructure disruption or geopolitical instability [15]. Integrating external context therefore enables predictive models to distinguish ordinary supplier variability from deterioration occurring within a broader environment of increasing disruption pressure.

3.4 Supplier Dependency and Network Exposure Features

Prediction of supplier failure probability is insufficient without understanding how strongly the organization depends on the affected supplier [18]. Dependency features should capture single-source relationships, supplier criticality, tier-one and tier-two connections, geographic concentration, alternative-source readiness, substitutability, and expected recovery difficulty. Supply relationships can be represented as a network:

$$G = (V, E)$$

where V contains suppliers, facilities, materials, technologies, and logistics nodes, and E represents dependency relationships between them. Network centrality can identify suppliers occupying structurally important positions through which disruption could propagate [21]. Shared upstream dependencies are particularly significant because apparently independent tier-one suppliers may rely on the same manufacturer, commodity source, technology platform, or transportation infrastructure [24]. Alternative-source readiness should also distinguish merely identified suppliers from technically qualified alternatives with sufficient capacity. Dependency intelligence consequently allows predictive risk to be interpreted according to potential organizational and network consequences [16].

3.5 Temporal Feature Engineering and Supplier-Specific Baselines

Raw observations should be transformed into temporal features that describe the direction and persistence of supplier change [17]. Rolling averages summarize recent conditions, while lag variables capture delayed relationships between deterioration indicators and subsequent disruption. Volatility measures distinguish stable performance from increasing uncertainty, and deterioration slopes quantify the direction and magnitude of change [20]. Recurrence counts identify repeated exceptions, whereas trend acceleration detects whether adverse movement is intensifying over time. Supplier-specific deviation may be expressed as:

$$Z_{i,t} = \frac{x_{i,t} - \mu_i^{base}}{\sigma_i^{base}}$$

where $x_{i,t}$ is the current observation and μ_i^{base} and σ_i^{base} represent the supplier's historical baseline [23]. Multivariate anomaly indicators can subsequently identify unusual combinations of financial, operational, cyber, commercial, or external behaviour that univariate thresholds may overlook.

3.6 Data Quality, Synchronization, and Leakage Prevention

Predictive reliability depends on consistent supplier identities and accurate temporal representation [19]. Missing observations require documented treatment, while duplicate records and inconsistent identifiers should be resolved through supplier-master and entity-matching controls. Different reporting frequencies must be synchronized without creating artificial observations [22]. Outliers should be investigated rather than automatically removed because extreme values may represent genuine deterioration. Most importantly, every variable should reflect its actual availability date. Information published after a historical prediction point must never enter that prediction, preventing temporal leakage and unrealistically inflated model performance [24].

Table 1. Multi-Domain Supplier Risk Data and Predictive Feature Architecture

Risk Domain	Representative Data	Engineered Feature	Update Frequency	Predictive Interpretation	Data Source
Financial	Liquidity, leverage, working capital, profitability, cash flow, credit status	Rolling ratios, deterioration slope, credit-change frequency	Monthly/quarterly	Emerging financial distress and reduced continuity capacity	Financial statements, credit data, supplier records
Commercial	Pricing, payments, contract amendments, order volumes, purchasing behaviour	Price volatility, payment deviation, contract-change recurrence	Daily/weekly	Commercial instability or changing supplier behaviour	ERP, procurement and contract systems
Operational	Capacity, output, downtime, fulfilment, service levels, quality defects	Capacity deviation, downtime persistence, fulfilment trend, defect acceleration	Daily/weekly	Weakening production or service capability	ERP, MES, QMS and supplier-performance systems
Logistics	Lead times, shipments, delays, transportation exceptions	Lead-time volatility, shipment-frequency change, delay recurrence	Near-real-time/daily	Increasing delivery instability and continuity exposure	TMS, carrier and shipment-tracking systems
Cybersecurity	Incidents, vulnerabilities, access anomalies, exposed services	Incident recurrence, vulnerability persistence, anomaly score	Near-real-time/daily	Increasing probability of digital disruption or compromise	SIEM, vulnerability and threat-intelligence systems
External	Sanctions, geopolitics, weather, commodities, infrastructure, regional economy	Event proximity, regional exposure, volatility, severity trend	Daily/event-driven	External pressure capable of amplifying supplier vulnerability	Regulatory, market, weather and external-risk feeds
Dependency	Criticality, sourcing, concentration, tier relationships, alternatives, shared dependencies	Centrality, concentration, substitutability, recovery difficulty	Monthly/event-driven	Potential magnitude and propagation of supplier disruption	Procurement, supplier-mapping and continuity systems

4. EXPLAINABLE AI FRAMEWORK FOR CONTINUOUS SUPPLIER RISK PREDICTION

4.1 Temporal Training and Supplier Risk Representation

Supplier-risk prediction should preserve the chronological structure through which deterioration becomes observable [25]. Historical data should therefore be partitioned into sequential training, validation, and testing periods rather than randomly distributed across datasets. Rolling prediction windows allow models to learn from preceding supplier histories while estimating disruption probability over defined future horizons, such as 7, 30, or 60 days [28]. Sequential observations capture whether financial, operational, cybersecurity, or logistics indicators are stable, deteriorating, or recovering. Each prediction at time t should use only information available at or before that point [31]. Consequently, supplier outcomes, revised financial statements, incident confirmations, or other information reported later must remain excluded from earlier feature windows. This temporal discipline prevents leakage and provides a realistic representation of prospective model performance [34].

4.2 Machine-Learning Models for Supplier Risk Prediction

Different machine-learning approaches provide complementary capabilities for supplier-risk prediction. Logistic regression offers a transparent baseline, efficient probability estimation, and readily interpretable coefficients but may inadequately represent complex nonlinear relationships [26]. Random forests capture nonlinearities and feature interactions while remaining comparatively robust to heterogeneous structured data [29]. Gradient boosting and XGBoost sequentially improve weak learners and can identify subtle combinations of deterioration signals across financial, operational, commercial, and external domains [32]. Support vector machines can model complex decision boundaries but may become computationally demanding for large supplier populations. Neural networks offer greater flexibility for high-dimensional and sequential relationships, although their complexity can reduce inherent interpretability [27]. Ensemble approaches combine complementary predictions:

$$\hat{P}_{i,t} = \sum_{m=1}^M w_m \hat{P}_{i,t}^{(m)}, \quad \sum_{m=1}^M w_m = 1$$

Model selection should therefore evaluate temporal robustness, probability calibration, computational cost, interpretability, stability across supplier categories, and warning lead time rather than predictive accuracy alone [33].

4.3 Anomaly Detection for Emerging and Unseen Risk Patterns

Historical disruption labels may be sparse, incomplete, or unrepresentative of future supplier failures, making anomaly detection an important complement to supervised prediction [25]. Isolation-based methods identify observations that can be separated from normal supplier behaviour with relatively few partitions, while clustering methods detect suppliers or periods departing from established peer structures [30]. Reconstruction-based models can identify unusual conditions through elevated reconstruction error when observed feature combinations differ substantially from learned normal patterns. Supplier-specific anomaly detection is particularly valuable because normal payment, delivery, capacity, and quality behaviour differs across organizations [34]. Multivariate approaches can additionally identify moderate deviations occurring simultaneously across several domains. Such anomaly evidence may reveal previously unseen deterioration patterns before sufficient labelled examples exist for conventional supervised learning [28].

4.4 Dynamic Supplier Risk Probability and Composite Scoring

Predictive models should generate continuously updated probabilities reflecting the likelihood of supplier disruption within a specified prediction horizon [27]. However, probability alone does not represent the operational significance of an adverse event. A dynamic composite score can therefore be expressed as:

$$DSR_{i,t} = P_{i,t} \times C_i \times D_i \times R_{i,t}$$

where $P_{i,t}$ represents predicted disruption probability, C_i operational criticality, D_i dependency exposure, and $R_{i,t}$ persistence or deterioration intensity. The scoring architecture should additionally incorporate prediction confidence and supplier substitutability [31]. A moderately risky single-source supplier with limited qualified alternatives may consequently warrant greater attention than a higher-probability supplier that can be replaced quickly. As financial results, delivery records, cyber events, external conditions, or dependency information change, both probability and composite exposure should be recalculated [29]. Continuous scoring therefore represents supplier risk as an evolving trajectory rather than a fixed rating assigned during periodic review.

4.5 Explainable Risk Attribution and Decision Transparency

Explainability should transform each supplier prediction from an opaque probability into an interpretable account of the factors influencing risk [26]. Global feature importance identifies variables that consistently influence predictions across the supplier population, supporting model validation and broader risk-policy development. Local explanations instead identify why a specific supplier received its current prediction [32]. SHAP-style attribution can decompose an individual model output into feature-level contributions:

$$f(x_i) = \phi_0 + \sum_{j=1}^p \phi_{ij}$$

where ϕ_0 represents the baseline prediction and ϕ_{ij} the contribution of feature j for supplier i . Risk-driver decomposition can aggregate these contributions into financial, operational, logistics, cybersecurity, commercial, and external domains [34]. Counterfactual reasoning can further indicate which plausible changes for example, improved fulfilment or reduced vulnerability persistence would materially lower predicted exposure. Explanations should present direction, magnitude, persistence, and confidence clearly enough for procurement and risk specialists to validate recommendations before consequential supplier decisions [30].

4.6 Dynamic Thresholds and Early-Warning Classification

Continuous predictions should be translated into operational warning states: Low, Emerging, Elevated, and Critical [25]. Low represents conditions within expected supplier behaviour, while Emerging identifies early deterioration requiring increased monitoring. Elevated indicates persistent or reinforcing risk requiring investigation and mitigation planning, whereas Critical signals substantial exposure requiring urgent resilience action [33]. Classification should combine probability thresholds with persistence, prediction confidence, supplier criticality, and uncertainty rather than relying on probability alone. Escalation rules should respond to sustained deterioration or rapidly accelerating exposure, while de-escalation should require sufficient evidence that adverse conditions have stabilized or recovered [28].

Figure 1. Explainable AI Architecture for Continuous Supplier Risk Assessment



5. RISK-GUIDED PROACTIVE MITIGATION AND SUPPLIER RESILIENCE

5.1 Connecting Explainable Risk Scores to Procurement Decisions

Explainable supplier-risk scores should translate predictive evidence into procurement actions that correspond with the source, persistence, and severity of deterioration [33]. Suppliers showing emerging financial or operational weakness may require increased review frequency, updated documentation, or direct engagement before purchasing restrictions are considered. Persistent deterioration can trigger procurement escalation, contract reassessment, revised purchasing limits, or closer monitoring of outstanding orders [36]. Explanations are particularly important because identical risk scores may arise from different underlying conditions. A supplier affected by temporary logistics disruption requires a different response from one experiencing sustained liquidity deterioration or cybersecurity weakness [39]. Procurement teams can therefore use risk-driver attribution to determine whether supplier discussions, corrective-action plans, sourcing adjustments, contractual protections, or strategic sourcing reviews are appropriate. This connects algorithmic prediction with evidence-based and proportionate procurement decisions.

5.2 Inventory Protection and Alternative Sourcing

Early warning creates an opportunity to protect operations before supplier deterioration becomes an actual shortage [34]. Where disruption probability increases, organizations can adjust safety-stock targets or build temporary inventory buffers for critical materials. Expedited procurement may be appropriate when sufficient supply remains available but future availability is uncertain [37]. For longer-term exposure, dual sourcing and supplier diversification can reduce dependence on vulnerable relationships. Alternative suppliers should be identified and technically qualified in advance because qualification requirements may prevent rapid substitution during disruption [40]. Production schedules can also be modified to prioritize products dependent on constrained components, while available inventory may be redistributed toward facilities facing greater exposure. Contingency sourcing should therefore reflect warning lead time, inventory coverage, alternative capacity, qualification requirements, and the expected duration of supplier deterioration [35].

5.3 Dependency-Aware Supplier Prioritization

Supplier prioritization should consider the consequences of disruption in addition to predicted probability. A prioritization function can be represented as:

$$SP_{it} = P_{it} \times C_i \times D_i \times NC_i \times R_i \times (1 - S_i)$$

where P_{it} is predicted disruption probability, C_i supplier criticality, D_i downstream dependency exposure, NC_i network centrality, R_i recovery difficulty, and S_i substitutability [33]. Inventory coverage should further modify intervention urgency because available stock determines how long operations can continue after supply interruption [38]. Consequently, a moderate-risk single-source supplier supporting mission-critical production with low inventory coverage and no qualified substitute may require earlier intervention than a high-risk supplier whose products can be replaced immediately [40]. Network centrality similarly identifies suppliers whose failure could affect several facilities or product lines. Dependency-aware prioritization therefore directs resilience resources toward suppliers presenting the greatest combination of vulnerability, operational consequence, and propagation potential [36].

5.4 Human Review and Intervention Decision Logic

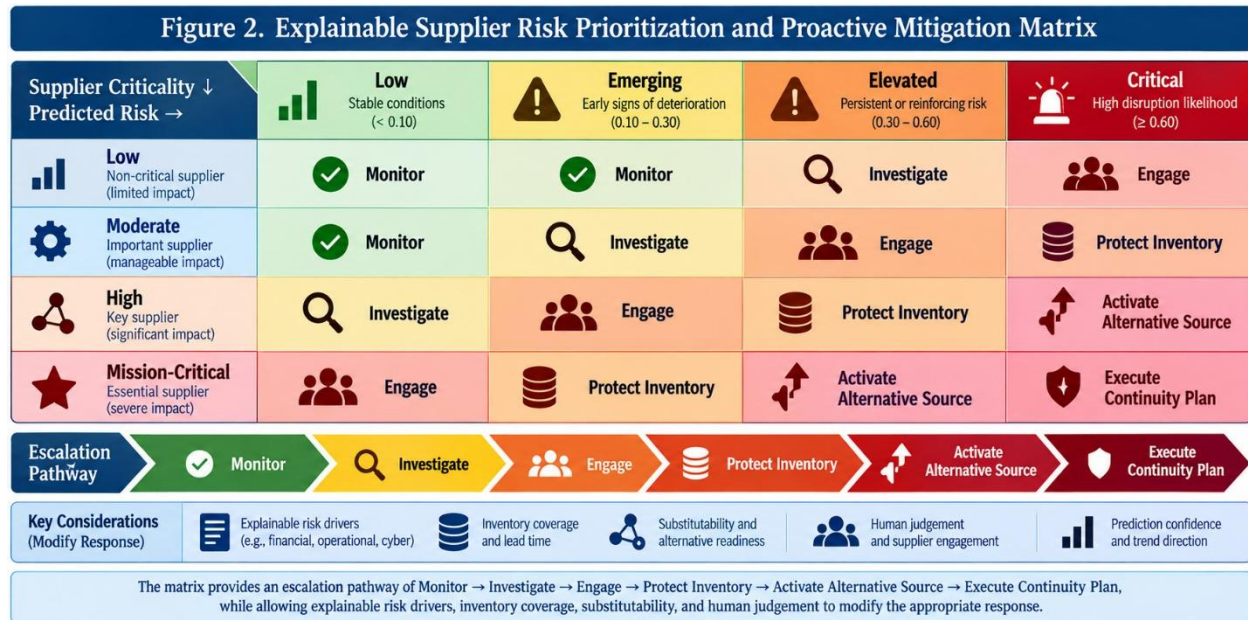
Predictive classifications should support rather than automatically determine consequential supplier decisions [34]. Human reviewers should examine model explanations, prediction confidence, supplier criticality, and the underlying evidence before approving escalation. Procurement specialists may also possess contextual information unavailable to the algorithm, including planned maintenance, temporary transportation constraints, contractual negotiations, or confirmed recovery measures [37]. Supplier engagement can clarify whether detected deterioration reflects genuine continuity risk or a known short-term condition. Decision authority should therefore be defined according to intervention severity, with higher-impact actions such as purchasing suspension, supplier replacement, or contract termination requiring appropriate organizational approval [39]. Documented review procedures, override rationales, and audit trails provide safeguards against unsupported automated adverse decisions while preserving accountability for intervention outcomes.

5.5 Closed-Loop Intervention and Adaptive Learning

Intervention outcomes should be returned to the analytical framework so that supplier-risk intelligence improves over time [35]. Outcome records should distinguish supplier recovery, continued deterioration, actual disruption, avoided shortages, successful substitution, and interventions that proved unnecessary. Mitigation effectiveness should also be evaluated because an anticipated disruption may not materialize precisely because preventive action was successful [38]. Feedback data can subsequently support probability recalibration, threshold adjustment, feature refinement, and periodic model retraining. Repeated false alarms may indicate overly sensitive thresholds, whereas missed disruptions can reveal insufficient features or poorly represented deterioration patterns [40]. Closed-loop learning therefore allows both prediction and intervention strategies to adapt using observed operational evidence.

5.6 Cascading Failure Prevention and Network Resilience

Supplier intervention should ultimately reduce the propagation of disruption across the wider supply network [33]. Multi-tier mapping can identify shared upstream suppliers, geographic clusters, critical-material dependencies, and common infrastructure capable of transmitting local failures across multiple relationships. Protecting strategically positioned suppliers or activating alternatives before disruption spreads can isolate vulnerable network segments [36]. Explainable, dependency-aware intervention therefore extends supplier-risk management beyond individual vendors toward containment of cascading operational exposure and broader network resilience.



6. MODEL EVALUATION, EXPLAINABILITY VALIDATION, AND RESPONSIBLE AI GOVERNANCE

6.1 Temporal Experimental Design and Validation

Evaluation should reproduce the chronological conditions under which supplier warnings would be generated in practice [36]. Historical observations should therefore be separated into training, validation, and untouched test periods rather than randomly partitioned. Rolling-window validation can assess performance as economic, operational, and supplier conditions change over time [39]. Strict availability timestamps should prevent future financial results, disruption outcomes, or revised supplier information from leaking into earlier predictions [42]. Evaluation should also stratify results across supplier size, sector, criticality, geographic exposure, and disruption category. Testing across stable and stressed periods determines whether predictive performance remains robust when economic conditions, transportation environments, or supplier operating patterns differ materially from those represented during training [45].

6.2 Predictive and Early-Warning Performance Metrics

Supplier-risk models should be evaluated according to both predictive discrimination and operational early-warning value [37]. Precision measures the proportion of generated alerts associated with genuine risk events, whereas recall captures the proportion of actual disruptions successfully identified. F1-score balances precision and recall, while ROC-AUC evaluates discrimination across classification thresholds [40]. PR-AUC is particularly informative where severe supplier disruptions are relatively uncommon. Specificity and false-positive rate quantify unnecessary escalation, while false-negative rate measures disruptions missed by the framework [43]. Probability calibration should determine whether predicted probabilities correspond with observed event frequencies. Warning lead time measures the interval between actionable detection and disruption, while actionable-warning rate identifies the proportion of warnings generated sufficiently early for procurement, inventory, sourcing, or continuity intervention [38].

6.3 Evaluating Explanation Quality and Decision Utility

Explanation quality should be assessed independently from predictive performance because an accurate model may still produce explanations that are unstable or operationally difficult to interpret [36]. Fidelity measures whether explanations accurately represent model behaviour, while consistency determines whether comparable supplier conditions generate comparable explanations. Stability examines whether minor input changes cause disproportionate changes in attributed risk drivers [41]. Feature-attribution analysis should verify whether financial, operational, cyber, logistics, and external contributions correspond with the underlying model response. Practitioner evaluation can additionally measure comprehensibility and actionability [44]. Procurement and risk specialists should be able to distinguish persistent deterioration from temporary abnormalities and understand

why escalation is recommended. Explanation utility is therefore demonstrated when interpretable evidence improves validation, intervention selection, and decision confidence rather than merely describing model outputs.

6.4 Benchmarking Against Conventional Supplier Assessment

Explainable continuous monitoring should be benchmarked against conventional supplier scorecards, questionnaires, static credit ratings, rule-based thresholds, scheduled audits, and manual procurement reviews [38]. Comparisons should use identical historical periods, supplier populations, disruption definitions, and prediction horizons to ensure methodological consistency. Conventional approaches may provide familiar governance and straightforward interpretation but can become outdated between assessment cycles [42]. Predictive AI can improve detection speed and data coverage, while explainable AI additionally connects predictions with interpretable risk drivers [45]. Comparative evaluation should therefore examine warning lead time, recall, false-negative exposure, adaptability, scalability, explanation usefulness, and intervention support rather than classification accuracy alone.

6.5 Governance, Fairness, Privacy, and Model Drift

Continuous supplier intelligence requires governance proportionate to the commercial sensitivity of financial, contractual, operational, and cybersecurity information [37]. Role-based access, data provenance controls, retention requirements, and audit trails should document how information and predictions are used. Performance should be examined across supplier sizes, industries, regions, and data-availability levels to identify systematic bias [40]. Human accountability remains necessary for consequential sourcing and contractual decisions. Model drift should be monitored when relationships between predictors and disruption outcomes change, while data drift should identify changes in underlying supplier characteristics [43]. Explanation monitoring can reveal unexpected changes in influential features. Periodic threshold recalibration, model validation, and retraining should therefore accompany deployment, with documented human approval ensuring responsible use of automated risk intelligence [44].

Table 2. Comparative Evaluation of Conventional and Explainable AI Supplier Risk Assessment

Evaluation Dimension	Conventional Assessment	Predictive AI	Explainable AI Framework	Resilience Implication
Detection timing	Periodic assessment cycles	Continuous probability estimation	Continuous prediction with interpretable early warnings	Increases time available for mitigation
Data coverage	Selected questionnaires and performance indicators	Broad multi-source datasets	Multi-domain data with attributed risk drivers	Provides wider visibility of deterioration
Adaptability	Static scores and predetermined review schedules	Models update with changing observations	Dynamic predictions, explanations, and thresholds	Responds to evolving supplier conditions
Interpretability	Generally transparent but limited in analytical depth	May be opaque for complex models	Global and supplier-specific explanations	Supports informed human validation
False-negative exposure	Emerging deterioration may remain undetected	Predictive patterns improve early detection	Predictions combined with anomaly evidence and explanations	Reduces risk of overlooked disruption
Intervention support	Relies heavily on manual judgement	Provides risk probability	Links probability to interpretable mitigation drivers	Enables proportionate proactive action
Scalability	Resource-intensive across large supplier populations	Automated portfolio-level monitoring	Scalable monitoring with prioritized explanations	Focuses attention on consequential suppliers
Auditability	Documented assessment records	Model outputs and performance records	Predictions, explanations, overrides, and interventions recorded	Strengthens accountability and governance

7. STRATEGIC IMPLICATIONS FOR UNITED STATES SUPPLY-NETWORK RESILIENCE

7.1 Procurement and Enterprise Risk Integration

Explainable supplier intelligence can connect strategic sourcing, supplier relationship management, procurement governance, enterprise risk management, and business continuity through a common representation of changing exposure [36]. Procurement teams can use risk drivers to prioritize supplier engagement, while continuity functions evaluate downstream consequences and alternative sourcing readiness [41]. Aggregated supplier-risk trajectories can also support executive reporting by identifying concentrations of vulnerability across critical materials, regions, technologies, and supplier categories [44].

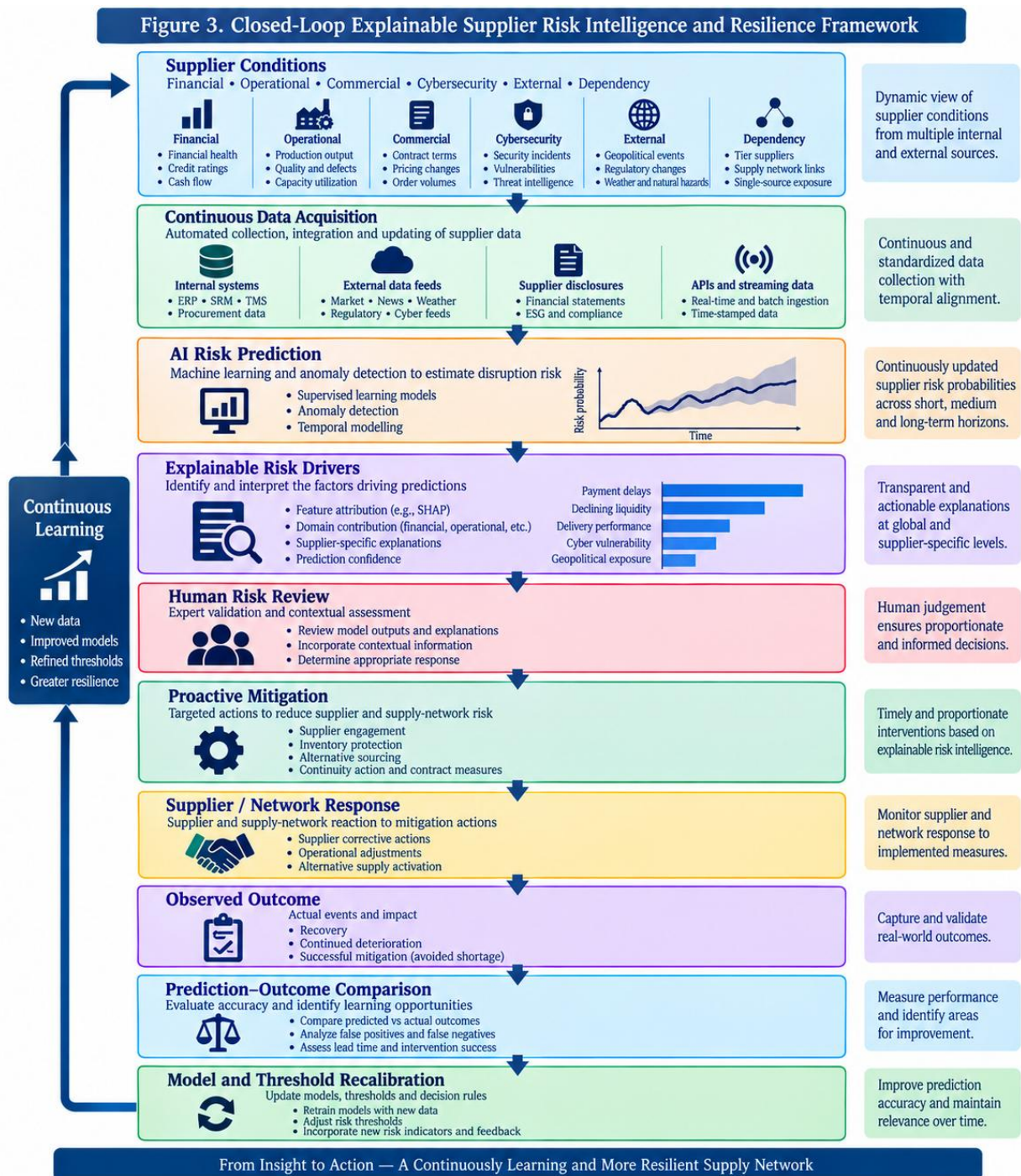
7.2 Implications for Critical and Interconnected Supply Networks

Continuous XAI has particular relevance for supply networks where third-party disruption can propagate rapidly across essential operations. Manufacturing organizations can identify vulnerable production dependencies, while healthcare and financial services can monitor critical suppliers supporting equipment, digital infrastructure, data, and specialized services [38]. Transportation, energy, and technology networks similarly depend on

interconnected physical and digital providers [42]. Dependency-aware prediction can reveal shared suppliers, infrastructure, technologies, and upstream relationships capable of transforming localized deterioration into broader operational disruption [45].

7.3 Organizational Adoption and Digital Transformation

Sustained adoption requires interoperable supplier-intelligence systems, standardized risk indicators, scalable data architecture, and cross-functional governance [39]. Responsible automation should preserve human accountability while allowing routine monitoring and prioritization to operate continuously. Organizations also require analytical capabilities for model validation, explanation review, data governance, and supplier-network mapping [43]. These capabilities enable XAI to become an embedded resilience function rather than an isolated analytical application.



8. CONCLUSION

8.1 Synthesis of Principal Findings

This article demonstrates how continuous multi-source monitoring can transform supplier-risk assessment from periodic observation into forward-looking intelligence. Integrating financial, commercial, operational, logistics, cybersecurity, external, and dependency information provides a comprehensive representation of changing supplier conditions. Temporal machine learning and anomaly detection identify emerging deterioration and unusual behavioural patterns, while dependency analysis establishes potential disruption consequences. Explainable risk attribution further reveals the specific factors driving predictions, enabling emerging supplier vulnerability to be identified and interpreted before operational disruption materializes.

8.2 Analytical and Resilience Contribution

The proposed framework advances supplier-risk management beyond static scores toward transparent, continuously updated, and intervention-oriented intelligence. By connecting predictive probabilities and explainable risk drivers with supplier criticality and operational decisions, it enables organizations to translate early warning into proportionate procurement, sourcing, inventory, and continuity actions.

8.3 Future Research Directions

Future research should investigate graph-based multi-tier modelling, multimodal XAI, streaming analytics, causal risk explanations, adaptive thresholds, and privacy-preserving supplier intelligence. Longitudinal evaluation should further establish how predictive interventions influence disruption prevention, supplier recovery, and sustained supply-network resilience.

REFERENCE

1. Elghomri B, Messaoudi F, Touti N. The Role of AI in Driving Accountability and Transparency in Global Supply Chains: The Fragmented Bridge Between Research and Practice. *Operations and Supply Chain Management: An International Journal*. 2025 Apr 19;18(2):275-87.
2. Jackson I, Ivanov D, Dolgui A, Namdar J. Generative artificial intelligence in supply chain and operations management: a capability-based framework for analysis and implementation. *International Journal of Production Research*. 2024 Sep 1;62(17):6120-45.
3. Muntala PS, Karri N. Enhancing Supply Chain Resilience with AI/ML in Oracle Fusion SCM. *American International Journal of Computer Science and Technology*. 2025 Jul 11;7(4):41-53.
4. Ahmed F, Rahman MM, Akter S. Reducing supply chain disruptions, costs, and waste using AI and blockchain to strengthen US economic resilience. *Journal of Tianjin University Science and Technology*. 2025;58:470-94.
5. Chukwunweike J. Coordinating PLC-based load shedding and variable-speed drives to prevent transformer overloading during industrial production peaks. *Int J Electr Data Commun*. 2025;6(2 Pt B):118-135. doi:10.22271/27083969.2025.v6.i2b.109.
6. Stanton DH. *The AI Revolution: Transforming Supply Chain Management: The Definitive Guide to Optimizing Procurement, Automating Production, and Mastering AI-Driven Global Logistics and Distribution*. Stanton Press; 2025 Aug 27.
7. Boone T, Fahimnia B, Ganesan R, Herold DM, Sanders NR. Generative AI: Opportunities, challenges, and research directions for supply chain resilience. *Transportation Research Part E: Logistics and Transportation Review*. 2025 Jul 1;199:104135.
8. Obunadike TC. Leveraging AI forecasting to quantify tariff-induced food price volatility in net-importing nations. *Int J Res Publ Rev*. 2025;6(6):12441-12458. doi:10.55248/gengpi.6.0625.23102.
9. Ishrat M, Khan W, Faisal SM. AI and risk forecasting: leveraging AI for environmental, social, and governance compliance. In *Artificial intelligence for financial risk management and analysis 2025* (pp. 307-334). IGI Global Scientific Publishing.
10. Chukwu N, Yufenyuy S, Ejiofor E, Ekweli D, Ogunleye O, Clement T, Obunadike C, Adeniji S, Elom E, Obunadike C. Resilient chain: AI-enhanced supply chain security and efficiency integration. *International Journal of Scientific and Management Research*. 2024;7(03):46-65.
11. Samuel Addo. Causal AI for strategic business planning: uncovering latent drivers of long-term organizational performance and resilience. *World Journal of Advanced Research and Reviews*, 2025, 26(2), 895-912. Article DOI: <https://doi.org/10.30574/wjarr.2025.26.2.1738>
12. Kilaru M, Potluri RM, Khan R. Application of explainable artificial intelligence (XAI) and blockchain technology in Indian sustainable, green supply chain management practices. In *Explainable AI and blockchain for secure and agile supply chains 2025* May 26 (pp. 129-141). Chapman and Hall/CRC.
13. Mukabbir MN. Explainable graph neural networks for malware propagation mapping in supply-chain attacks. *Frontiers in Computer Science and Artificial Intelligence*. 2025 Nov 18;4(1):47-60.
14. Ogan RK. Machine-learning framework for predicting point-of-sale integration failures across digital ordering, payment, and third-party delivery technology ecosystems. *Int J Res Publ Rev*. 2025;6(12):8887-8898.
15. Diaz R, Smith K, Ungo R. A Cyber Risk Management Perspective on Shipbuilding AI-Based Supply Chain Management. *Journal of Information Warfare*. 2024 Oct 1;23(4):57-71.
16. Effah D, Bai C, Asante WA, Quayson M. The role of artificial intelligence in coping with extreme weather-induced cocoa supply chain risks. *IEEE Transactions on Engineering Management*. 2023 Jul 19;71:9854-75.
17. Racheal Kikachukwu Ogan. (2023). AUTOMATED CONFIGURATION COMPLIANCE ANALYTICS FOR DETECTING OPERATIONAL DRIFT AND PREVENTING SERVICE DEGRADATION ACROSS MULTI-LOCATION RESTAURANT TECHNOLOGY SYSTEMS. *INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)*, 07(12), 807-819. <https://doi.org/10.5281/zenodo.22267240>
18. Chowdhury AR. A systematic review of risk-based procurement strategies in retail supply chains: Sourcing flexibility and vendor disruption management. *American Journal of Advanced Technology and Engineering Solutions*. 2025 Apr 17;1(01):466-505.
19. Kosasih EE, Margaroli F, Gelli S, Aziz A, Wildgoose N, Brintrup A. Towards knowledge graph reasoning for supply chain risk management

- using graph neural networks. *International Journal of Production Research*. 2024 Aug 2;62(15):5596-612.
20. Magajiaka J, Adesanmi B. Lifecycle cost and resilience performance evaluation of climate-resilient urban road infrastructure under climate risk scenarios. *International Journal of Current Research*. 2026;18(5):37242-37251.
 21. Teixeira AR, Ferreira JV, Ramos AL. Intelligent supply chain management: A systematic literature review on artificial intelligence contributions. *Information*. 2025 May 13;16(5):399.
 22. Singh RK, Modgil S, Shore A. Building artificial intelligence enabled resilient supply chain: a multi-method approach. *Journal of Enterprise Information Management*. 2024 Apr 22;37(2):414-36.
 23. Racheal Kikachukwu Ogan. Machine-learning-based API failure prediction and root-cause analytics for improving reliability of enterprise banking integration architectures at scale. *Int J Comput Artif Intell* 2021;2(2):142-153. DOI: [10.33545/27076571.2021.v2.i2a.378](https://doi.org/10.33545/27076571.2021.v2.i2a.378)
 24. Faruk MI, Plabon FW, Saha US, Hossain MD. AI-driven project risk management: Leveraging artificial intelligence to predict, mitigate, and manage project risks in critical infrastructure and national security projects. *Journal of Computer Science and Technology Studies*. 2025 Jun 12;7(6):123-37.
 25. Herath S, Johannsson JG, Shrestha YR, von Krogh G. Supply Chain Resilience Through Artificial Intelligence-Enabled Predictive Maintenance: A Design Science Research Study. Available at SSRN 5153658. 2025 Feb 25.
 26. Ogan RK. Risk-based API governance for predicting integration failures, security anomalies, and service degradation across hybrid enterprise application environments. *Int J Finance Manage Econ*. 2024;7(2):871-882. doi:10.33545/26179210.2024.v7.i2.946.
 27. Jauhar SK, Harinath S, Krishnaswamy V, Paul SK. Explainable artificial intelligence to improve the resilience of perishable product supply chains by leveraging customer characteristics. *Annals of Operations Research*. 2025 Nov;354(1):103-42.
 28. Kinney AB. Leveraging Artificial Intelligence for Supply Chain Risk Management. Institute for Homeland Security; 2024.
 29. Ethel Esinam Atubrah. CLIMATE ADAPTATION POLICY AND COMMUNITY RESILIENCE: CULTURAL IDENTITY, LIVELIHOODS, AND ENVIRONMENTAL DISPLACEMENT. *International Journal of Science and Research Archive*, 2026, 20(02), 356–370. Article DOI: <https://doi.org/10.30574/ijrsra.2026.20.2.1635>.
 30. Sadeghi K, Ojha D, Kaur P, Mahto RV, Dhir A. Explainable artificial intelligence and agile decision-making in supply chain cyber resilience. *Decision Support Systems*. 2024 May 1;180:114194.
 31. Shah HM, Gardas BB, Narwane VS, Mehta HS. The contemporary state of big data analytics and artificial intelligence towards intelligent supply chain risk management: a comprehensive review. *Kybernetes*. 2023 May 5;52(5):1643-97.
 32. MGBAJIACA, JOHNBOSCO. 2025. "Co-Designing Resilient Infrastructure: Participatory Approaches for Sustainable Implementation". *Current Journal of Applied Science and Technology* 44 (8):11-17. <https://doi.org/10.9734/cjast/2025/v44i84586>.
 33. Brintrup A, Kosasih E, Schaffer P, Zheng G, Demirel G, MacCarthy BL. Digital supply chain surveillance using artificial intelligence: definitions, opportunities and risks. *International Journal of Production Research*. 2024 Jul 2;62(13):4674-95.
 34. Aljohani A. Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. *Sustainability*. 2023 Oct 20;15(20):15088.
 35. Ogunsola O, Serh LZ, Hutchful N. Adaptive AI Systems for Intelligent Decision Optimization in Supply Chain Management: A Machine Learning Approach. *Journal Of Engineering And Computer Sciences*. 2025 Dec 3;4(12):10-8.
 36. Nimmy SF. *Explainable artificial intelligence in supply chain operational risk management (XAI-SCORM): A comprehensive approach towards interpretability, transparency, and trustworthiness* (Doctoral dissertation, University of New South Wales (Australia)).
 37. Rane J, Chaudhari RA, Rane NL. Enhancing sustainable supply chain resilience through artificial intelligence and machine learning: Industry 4.0 and Industry 5.0 in manufacturing. Deep Science Publishing; 2025 Jul 26.
 38. Iqbal U. AI-powered supplier risk intelligence: Predicting financial and geopolitical supply chain disruptions in US critical industries. *Journal of Engineering and Computational Intelligence Review*. 2025 Jul 31;3(2):173-93.
 39. Sumi SS. Implementation of explainable AI-driven framework for supply chain optimization: A practical case study in industrial engineering. *International Journal of Scientific Interdisciplinary Research*. 2025 Dec 16;6(2):143-72.
 40. Hasan MR, Rahman MA, Gomes CA, Nitu FN, Gomes CA, Islam MR, Shawon RE. Building robust AI and machine learning models for supplier risk management: A data-driven strategy for enhancing supply chain resilience in the USA. *Advances in Consumer Research*. 2025 Jul 1;2(4):1152-71.
 41. Ordibazar AH, Hussain OK, Chakraborty RK, Irannezhad E, Saberi M. Artificial intelligence applications for supply chain risk management considering interconnectivity, external events exposures and transparency: a systematic literature review. *Modern Supply Chain Research and Applications*. 2025 Aug 26;7(2):148-79.
 42. Jahin MA, Naife SA, Saha AK, Mridha MF. Ai in supply chain risk assessment: A systematic literature review and bibliometric analysis. *arXiv preprint arXiv:2401.10895*. 2023 Dec 12.
 43. Nsama F. Strategic development of AI-driven supply chain resilience frameworks for critical US sectors. *Communication In Physical Sciences*. 2025 Oct 13;12(5):1538-60.
 44. Li X, Krivtsov V, Pan C, Nassehi A, Gao RX, Ivanov D. End-to-end supply chain resilience management using deep learning, survival analysis, and explainable artificial intelligence. *International Journal of Production Research*. 2025 Feb 1;63(3):1174-202.
 45. Sarker B. Leveraging machine learning for supply chain disruption prediction and risk assessment in US industries. *International Journal of Applied Mathematics*. 2025 Nov 2;38(10s):2382-410.