IJECS Open Access https://ijecs.in
International Journal of Engineering and Computer Science
Volume 15, Issue 07, July 2026, Page No. 28678-28688
ISSN: 2319-7242 DOI: 10.18535/ijecs.v15i07.5585

Cognitive Supplier Risk Management Systems for Medical Device: AI Framework for Predictive Quality, Compliance, and Supply Chain Resilience

Binitkumar M Vaghani[1]

MS in Mechanical Engineering, United Sates

Abstract:
Medical device manufacturers depend on complex supplier networks for critical components, materials, software, and production services. Failures within these networks can create serious quality defects, regulatory non-compliance, supply interruptions, delayed product availability, and potential risks to patient safety. Traditional supplier risk management approaches are often retrospective, fragmented across quality and procurement systems, and insufficiently responsive to emerging disruptions. This study develops a cognitive supplier risk management framework that applies artificial intelligence to integrate predictive quality monitoring, compliance intelligence, and supply chain resilience planning. The proposed framework combines supplier audit findings, non-conformance records, corrective and preventive action data, delivery performance, regulatory indicators, logistics signals, and external disruption data to generate dynamic supplier risk scores. It uses predictive analytics, anomaly detection, natural language processing, and decision-support dashboards to identify early warning signs of supplier instability and recommend targeted mitigation actions. The framework also incorporates digital supply chain twin capabilities to support scenario analysis, supplier substitution planning, and recovery decision-making during disruptions. The study contributes a structured model for linking AI-enabled supplier intelligence with medical device quality management and regulatory governance. It emphasizes that human oversight, data quality, explainability, validation, and accountability remain essential for responsible implementation. The framework offers practical value for procurement, quality assurance, regulatory affairs, and supply chain leadership seeking to improve supplier visibility, compliance readiness, and operational resilience.

Keywords: Cognitive supplier risk management, medical device supply chains, artificial intelligence, predictive quality, regulatory compliance, supply chain resilience, digital supply chain twin..

1. Introduction

1.1 Background of the Study

Medical device manufacturing increasingly depends on complex, global, and specialized supplier networks. Contemporary devices combine electronic parts, software-enabled systems, sensors, sterilized materials, packaging inputs, precision-engineered components, and outsourced manufacturing services from several supplier tiers. This structure helps manufacturer's access technical expertise, reduce costs, scale production, and respond to market demand. However, it increases exposure to supplier-related risks because critical activities occur outside the direct control of the original equipment manufacturer. In the medical device sector, supplier performance is not only an operational issue; it is also connected to regulatory compliance, product quality, and patient safety. A defective component, delayed material, undocumented process change, or weak supplier quality system can affect the safety, effectiveness, and availability of finished devices.

The growth of digital manufacturing, outsourced production, and interconnected supply systems has made supplier risk management more demanding. Traditional methods such as periodic audits, manual scorecards, and retrospective performance reviews are too slow to detect emerging risks. Supply risk may arise from uncertainty in supplier capacity, quality consistency, delivery reliability, compliance behavior, financial stability, or exposure to external disruption (Zsidisin, 2003). For medical device manufacturers, these risks are intensified by regulated quality systems, traceability obligations, documentation control, and the need to prove that purchased products and services meet defined requirements. Medical device regulation is linked to protecting patients from unsafe or ineffective technologies, which means supplier failures can become regulatory and clinical concerns (Maisel, 2004).

1.2 Problem Statement

Despite the strategic role of suppliers, many medical device firms manage supplier risk reactively. Problems are often detected only after non-conformances, late deliveries, failed audits, complaints, production stoppages, or regulatory concerns have occurred. This approach is inadequate in an industry where quality and compliance failures can lead to recalls, warning letters, approval delays, loss of market access, reputational damage, and patient harm. Supplier disruption may also threaten production continuity, especially when devices depend on single-source components, specialized materials, validated manufacturing processes, or geographically concentrated suppliers.

Research on supply chain disruption shows the importance of proactive systems that identify vulnerabilities before they become failures (Blackhurst et al., 2005; Kleindorfer & Saad, 2005). Christopher and Peck (2004) argue that resilience requires visibility, flexibility, collaboration, and rapid response capacity. These principles are relevant to medical device supply chains because resilience must be balanced with strict quality and regulatory controls. A medical device manufacturer cannot simply replace a supplier without supplier qualification, process validation, documentation updates, and possible regulatory review. Supplier risk in this sector is therefore a combined quality, compliance, operational, and resilience problem.

Global supply chain risk literature shows that internationally distributed supplier networks face transportation delays, political instability, natural disasters, demand volatility, supplier opportunism, and information asymmetry (Manuj & Mentzer, 2008). Ho et al. (2015) explain that supply chain risk management requires systematic risk identification, assessment, mitigation, and monitoring across the supply network. However, many existing supplier risk systems do not provide the predictive intelligence needed to connect quality signals, compliance indicators, delivery behavior, and external disruption data. This creates a gap for manufacturers that need earlier warnings, stronger supplier visibility, and evidence-based prioritization.

1.3 Research Aim

The aim of this study is to develop a cognitive AI-based supplier risk management framework for the medical device industry. The framework is designed to support prediction of supplier-related quality failures, compliance risks, and supply chain disruptions by integrating supplier performance data, quality records, audit findings, regulatory indicators, delivery patterns, and external risk signals. Rather than treating supplier risk as a static scorecard exercise, the study positions risk management as a continuous learning process supported by artificial intelligence, predictive analytics, and human oversight.

1.4 Research Objectives

This study has five objectives. First, it examines supplier risk factors affecting medical device supply chains, including quality inconsistency, non-compliance, delivery instability, limited capacity, disruption exposure, and weak documentation control. Second, it identifies how artificial intelligence and predictive analytics can improve early detection of supplier-related risks by analyzing quality events, audit outcomes, corrective actions, delivery performance, and external risk data. Third, it develops a cognitive supplier risk management framework that combines data integration, risk prediction, compliance intelligence, supplier scoring, and decision support. Fourth, it links predictive quality, compliance monitoring, and resilience planning into a unified model that reflects regulated medical device manufacturing. Fifth, it provides practical implications for manufacturers, regulators, procurement teams, quality managers, and supply chain leaders.

1.5 Research Questions

This study is guided by four research questions. First, what supplier risk factors most affect quality, compliance, and resilience in medical device supply chains Second, how can artificial intelligence improve early detection of supplier-related quality and regulatory risks Third, what components should be included in a cognitive supplier risk management system for medical device manufacturers Fourth, how can predictive supplier intelligence strengthen supply chain resilience while supporting patient safety, production continuity, and regulatory compliance?

2. Literature Review and Conceptual Foundations

2.1 Supplier Risk Management in Regulated Supply Chains

Supplier risk refers to the possibility that a supplier's weakness, failure, or instability will affect a manufacturer's quality, cost, delivery, compliance, or customer service. In medical device supply chains, this risk is intensified because purchased components, materials, software, packaging, and outsourced processes may influence patient safety and regulatory conformity. Tang (2006) explains that supply chain risk involves operational uncertainty and major disruption exposure, while Wagner and Bode (2008) show that supply-side risk can reduce delivery, quality, and flexibility performance. Supplier risk includes disruption risk, operational risk, demand risk, and supply continuity risk. Disruption risk covers events such as supplier shutdowns, transport failure, geopolitical instability, natural disasters, or shortages. Operational risk concerns routine failures in production, inspection, documentation, delivery, or process control. Demand risk occurs when clinical or market demand changes faster than suppliers can respond. Supply continuity risk concerns whether approved suppliers can provide compliant components consistently without delay, unauthorized substitution, or quality drift.

2.2 Medical Device Quality and Regulatory Risk

Supplier risk management in medical devices must go beyond price and delivery because supplier performance can affect device safety and regulatory approval. Supplier qualification is essential. Manufacturers must confirm that suppliers have suitable technical capability, process controls, quality systems, and documentation practices. Component traceability is equally important because materials, electronic parts, sterile packaging, and software elements may need to be linked to batches, complaints, field actions, or recalls. Regulatory documentation, including certificates, specifications, audit reports, change-control files, and corrective and preventive action records, provides evidence that supplier processes remain controlled. Weak documentation can create compliance exposure even when the product appears acceptable. Audit readiness matters because manufacturers must show continuing supplier oversight. Post-market quality surveillance closes the loop by connecting complaints, defects, adverse events, and field performance data back to supplier processes.

2.3 Supply Chain Resilience Theory

Supply chain resilience is the ability to prepare for, respond to, recover from, and adapt after disruption. Pettit et al. (2010) define resilience through the balance between vulnerabilities and capabilities, while Hohenstein et al. (2015) identify visibility, flexibility, collaboration, and recovery as central themes. Ali et al. (2017) show that resilience is not only a response after disruption but also a capability built before disruption occurs. For medical device firms, resilience depends on supplier visibility, flexible sourcing, redundancy for critical parts, collaboration, recovery capacity, and adaptive response. Visibility helps detect early warning signals. Flexibility allows sourcing or production changes. Redundancy protects critical supply. Collaboration supports joint problem-solving, while recovery capacity determines how quickly supply returns to acceptable performance.

2.4 AI, Big Data, and Predictive Analytics in Supply Chain Management

AI, big data, and predictive analytics are moving supplier risk management from periodic review toward continuous risk intelligence. Waller and Fawcett (2013) argue that data science and predictive analytics can transform supply chain design and decision-making. Hazen et al. (2014), however, stress that analytics depends on data quality, since incomplete or inaccurate data can lead to poor decisions. Big data analytics enables firms to combine supplier scorecards, audit findings, non-conformance records, delivery data, financial indicators, logistics signals, and external disruption alerts. Wang et al. (2016) show that big data improves visibility and decision support, while Kache and Seuring (2017) note that digital information creates opportunities and governance challenges. AI techniques such as machine learning, anomaly detection, and natural language processing can identify supplier deterioration earlier than traditional review cycles. Min (2010) highlights AI applications in supply chain planning and control, while Toorajipour et al. (2021) confirm its role in forecasting, supplier selection, and risk analysis. Baryannis et al. (2019) link AI and predictive analytics to risk prediction and preventive action.

2.5 Cognitive Supplier Risk Management

Cognitive supplier risk management describes an AI-enabled system that learns from supplier data, detects changing risk patterns, predicts emerging quality or compliance threats, and recommends mitigation actions. Unlike static scorecards, a cognitive system can integrate internal quality data, supplier audits, delivery records, regulatory signals, and external risk intelligence. It can then generate risk scores, explain risk drivers, flag weak suppliers, and support decisions such as intensified audits, dual sourcing, corrective action escalation, or inventory buffering. In medical device manufacturing, this approach is valuable because it connects predictive quality, compliance monitoring, and resilience planning within one decision-support structure.

Table 1 Summary of Key Literature

Author(s)	Focus	Contribution	Relevance
Pettit et al.; Hohenstein et al.; Ali et al.	Resilience	Explain capabilities and adaptive response	Supports resilience
Tang; Wagner and Bode	Risk	Clarify disruption and performance risks	Defines risk categories
Waller and Fawcett; Hazen et al.; Wang et al.; Kache and Seuring	Analytics	Link data quality, big data, and decisions	Supports prediction
Min; Baryannis et al.; Toorajipour et al.	AI	Show AI use in forecasting and risk prediction	Justifies cognitive AI

3. Methodology and Research Design

3.1 Research Approach

This study adopts a conceptual framework development approach supported by structured literature synthesis and scenario-based risk modelling. It integrates supply chain risk, medical-device quality management, predictive analytics, and AI governance into a decision-support framework. The framework combines internal supplier data with external intelligence to identify threats before they cause defects, non-compliance, disruption, or patient-safety concerns.

The literature synthesis identifies capabilities needed for intelligent supplier risk management. Predictive analytics can reshape supply-chain design and operational decisions (Waller & Fawcett, 2013), but its value depends on data that are complete, consistent, timely, and decision-relevant (Hazen et al., 2014). The system cycle is: collect and validate data, detect patterns, predict risk, recommend mitigation, and review performance. Scenarios include rising component defects, overdue corrective actions, adverse inspection findings, and critical-supplier disruption.

3.2 Data Sources for the Proposed AI System

The proposed system integrates data from quality systems, enterprise resource planning platforms, supplier portals, and external intelligence feeds. Supplier risk is rarely visible through one measure; a supplier may meet delivery targets while presenting major compliance risk through repeated audit observations or delayed corrective actions.

Internal data include supplier audit reports, non-conformance reports, corrective and preventive action (CAPA) records, incoming inspection findings, defect rates, delivery performance, production disruption data, complaints, and recalls. Audit and CAPA records indicate quality-system maturity, recurring failures, and responsiveness. Inspection and defect data flag component, documentation, packaging, sterility, or process problems. Delivery data identify lead-time volatility, missed commitments, and fulfilment reliability.

External variables include supplier financial health, credit alerts, ownership changes, political instability, trade restrictions, natural-hazard exposure, transport congestion, weather events, cybersecurity alerts, and regulatory notices. Combining heterogeneous sources reflects the potential and implementation difficulty of big-data-enabled supply-chain management (Kache & Seuring, 2017; Wang et al., 2016). Data ingestion should use common supplier identifiers, time stamps, access controls, and validation checks to avoid misleading inputs.

3.3 Risk Dimensions

The framework classifies supplier risk into seven connected dimensions. Quality risk includes defective materials, process variation, weak change control, poor traceability, and recurring

non-conformances. Compliance risk covers audit observations, incomplete documentation, overdue CAPAs, and regulatory exposure. Delivery risk concerns late deliveries, lead-time variation, capacity constraints, and logistics unreliability. Financial risk captures liquidity deterioration, credit warnings, pricing instability, and supplier fragility.

Operational risk covers capacity limits, equipment downtime, workforce shortages, single-source reliance, and inadequate continuity planning. Cybersecurity risk includes compromised digital records, insecure data exchange, ransomware exposure, and vulnerable systems. Disruption risk covers geopolitical events, natural disasters, public-health emergencies, transport interruptions, and supplier-site incidents. The system should provide individual scores and an integrated profile because the dimensions interact. Financial decline, for example, may increase both quality and delivery risk.

3.4 Analytical Method

The analytical layer combines predictive analytics, risk scoring, anomaly detection, natural language processing (NLP), and dashboard-based decision support. Predictive analytics estimates the probability of quality non-conformance, late delivery, audit failure, or supply interruption within a specified period. Suitable methods include supervised machine learning, time-series forecasting, and classification algorithms.

A transparent risk-scoring model converts indicators into comparable supplier ratings. Each dimension can be scored from 0 to 100, with higher values representing greater risk. Weights should be set with input from quality assurance, regulatory affairs, procurement, manufacturing, and supply-chain personnel, then adjusted for component criticality. Anomaly detection can flag sudden inspection failures, abnormal delivery delays, or unusual CAPA closure patterns.

NLP can analyse audit narratives, supplier correspondence, deviation investigations, and regulatory observations. It can extract recurring themes, classify finding severity, and identify language suggesting deteriorating controls. Yet AI outputs should support, not replace, professional judgement. Their value depends on integration into real workflows and actionable information for users (Kelly et al., 2019). Dashboards should display overall score, risk drivers, predicted trend, confidence level, recommended action, and supporting evidence.

3.5 Ethical and Regulatory Considerations

Robust governance is essential because the system may inform supplier approval, audit frequency, purchasing decisions, and continuity planning. Model documentation should define intended use, data sources, prediction targets, performance measures, limitations, and escalation processes. Explainability is necessary because users must understand why a supplier is classified as high risk and which indicators drive the result. This reflects governance principles for accountability and oversight in healthcare AI use (Reddy et al., 2020).

Missing, biased, outdated, or inconsistently coded records can create inaccurate estimates and unfairly penalise suppliers. The system should assess completeness, accuracy, representativeness, and data drift while retaining audit trails for updates and outputs. Bias monitoring should prevent unfair disadvantage from regional data gaps or reporting formats. Consistent with responsible machine-learning guidance, qualified personnel should oversee design, validation, implementation, and post-deployment monitoring (Wiens et al., 2019). Final decisions on supplier suspension, product release, regulatory reporting, and patient-safety actions must remain with authorised human decision-makers.

Table 2 Supplier Risk Indicators for Medical Device Supply Chains

Risk Category	Illustrative Indicator	Principal Data Source	AI Method	Expected Output
Quality risk	Defect rate; recurring non-conformances	Inspection records; NCR database	Classification; anomaly detection	Quality-failure likelihood
Compliance risk	Open CAPAs; documentation gaps	CAPA system; audit reports	NLP; risk scoring	Compliance exposure score
Delivery risk	Late delivery; lead-time variance	ERP records; logistics feeds	Time-series forecasting	Delay probability
Financial risk	Credit deterioration; ownership change	Financial reports; credit alerts	Predictive scoring	Financial-stability rating
Operational risk	Capacity constraint; downtime	Supplier surveys; production records	Scenario modelling	Continuity-risk estimate
Cybersecurity risk	Security incident; access anomaly	Security logs; supplier assessments	Anomaly detection	Vulnerability alert
Disruption risk	Flood, trade restriction, congestion	Environmental and logistics feeds	Event detection; scenario modelling	Disruption probability

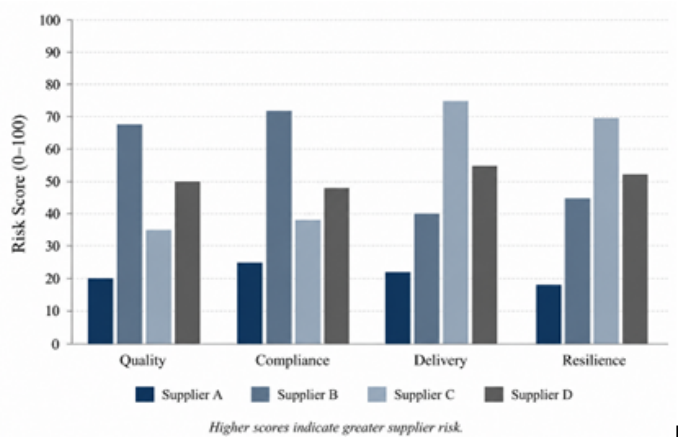

Figure 1 *Illustrative Supplier Risk Scoring Model Across Quality, Compliance, Delivery, and Resilience Dimensions*

4. Proposed Cognitive AI Framework for Supplier Risk Management

4.1 Framework Overview

The proposed Cognitive Supplier Risk Management System (CSRMS) converts dispersed supplier information into risk intelligence for medical device manufacturers. It moves beyond scorecards by combining operational, quality, regulatory, and external evidence to detect threats before they cause quality, compliance, or continuity failures. The design reflects Industry 4.0 and intelligent decision support (Lee et al., 2015; Kusiak,

2018), together with the expanding application of artificial intelligence to supply-chain prediction and optimisation (Baryannis et al., 2019; Toorajipour et al., 2021).

The CSRMS contains five connected layers: data acquisition and integration; data quality and governance; AI-based risk detection; compliance and quality intelligence; and decision support with resilience planning. Feedback from audits, mitigation actions, and supplier outcomes updates risk estimates and recommendations.

4.2 Layer 1: Data Acquisition and Integration

The first layer creates a supplier-risk data environment. Structured data are obtained from enterprise resource planning, manufacturing execution, quality management, procurement, supplier-portal, and logistics systems. Indicators include fulfilment, inspection results, defect rates, deviations, CAPA status, batch-release outcomes, inventory, and shipment delays. Medical device manufacturers should also include qualification files, audit findings, certificates, change-control records, complaints, and field-performance signals.

Unstructured information adds context. The system can ingest audit narratives, supplier correspondence, inspection observations, regulatory notices, recall reports, news, weather alerts, geopolitical developments, and financial-risk feeds. AI-driven supply-chain management is more effective when internal and external data are connected rather than reviewed separately (Min, 2010; Baryannis et al., 2019). Common supplier identifiers, interoperable standards, application programming interfaces, and time-stamped records link quality performance with commercial, logistical, and regulatory conditions.

4.3 Layer 2: Data Quality and Governance

The second layer ensures analytical reliability through cleaning, de-duplication, completeness checks, outlier review, unit harmonisation, and master-data management. Supplier names, component codes, defect categories, audit classifications, and CAPA labels must be standardised across sites; otherwise, inconsistent records can distort predictions. Data quality is a precondition for credible predictive analytics in supply chains (Hazen et al., 2014).

Governance defines ownership, access rights, retention rules, model documentation, and auditable decision logs. Each risk score should be traceable to its inputs, model version, and generation date. Validation should test performance across supplier categories, product classes, and locations. In medical devices, where AI-supported actions may affect safety and compliance, transparency, accountability, human oversight, and continuous monitoring are indispensable (Gerke et al., 2020; Benjamens et al., 2020).

4.4 Layer 3: AI-Based Risk Detection

The third layer converts governed data into early-warning intelligence. Supervised models estimate the probability of late delivery, material rejection, repeat non-conformance, audit failure, or disruption from historic patterns. Unsupervised anomaly detection flags unusual movements in defects, lead-time volatility, CAPA closure duration, shipment behaviour, or documentation activity.

Pattern-recognition models group suppliers with comparable risk profiles and show connections among quality events, component criticality, single-source exposure, and geographic concentration. Natural language processing can assess audit reports, supplier responses, complaint narratives, and regulatory communications for inadequate validation, incomplete traceability, delayed corrective action, or weak process control. Every alert should show confidence, the affected component or process, principal drivers, and supporting evidence. AI is most valuable when it strengthens managerial judgement rather than replaces it (Toorajipour et al., 2021).

4.5 Layer 4: Compliance and Quality Intelligence

The fourth layer translates detected signals into medical-device-specific quality and compliance intelligence. It identifies suppliers whose patterns suggest likely non-conformance, overdue CAPAs, missing certificates, incomplete change notifications, repeated audit observations, or weak document control. For example, increased inspection failures combined with overdue CAPAs and an approaching certificate-expiry date should produce a higher risk classification than any single indicator alone.

Prioritisation should consider component criticality, patient-safety relevance, regulatory status, and alternative-source availability. Recommended actions may include targeted audits, enhanced inspection, supplier development, temporary approval restrictions, or secondary-supplier qualification. This system-level approach aligns with the need to address performance, safety, and accountability together in medical-device AI governance (Gerke et al., 2020).

4.6 Layer 5: Decision Support and Resilience Planning

The final layer provides dashboards for procurement, quality assurance, regulatory affairs, and operations. They rank suppliers, show trends and alert drivers, and monitor mitigation actions. Suppliers may be stable, watch-list, high-risk, or critical, with evidence-linked interventions.

Scenario tools test the implications of supplier failure, regulatory restriction, transport delays, or material shortages. Linked with a digital supply-chain twin, the framework can simulate alternate sourcing, inventory buffers, production reallocation, and recovery times. Digital twins model dependencies and resilience options (Ivanov & Dolgui, 2021). The CSRMS therefore shifts supplier management from delayed reporting to anticipatory quality, compliance, and resilience planning.

Table 3 Components of the Cognitive Supplier Risk Management Framework

Framework Layer	Function	Data Input	AI Technique	Decision Output	Managerial Use
Data acquisition	Integrate evidence	ERP, QMS, audits, logistics	Integration, matching	Supplier profile	Visibility
Governance	Assure reliable records	Master data, quality records	Validation, anomaly screening	Trusted dataset	Audit readiness
Risk detection	Identify emerging risk	History, audit text, disruptions	Prediction, NLP, clustering	Early-warning alerts	Preventive action
Compliance and quality	Assess exposure	CAPAs, certificates, non-conformances	Risk scoring, rules	Compliance priority	Audit or sourcing action

Framework Layer	Function	Data Input	AI Technique	Decision Output	Managerial Use
Decision and resilience	Select recovery options	Risk scores, inventory, network data	Optimisation, digital twin	Ranked suppliers, scenarios	Resilience planning

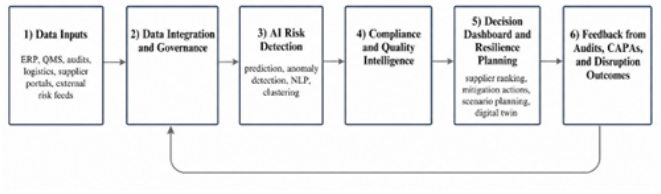

Figure 2 *Cognitive AI Framework for Predictive Supplier Risk Management*

5. Predictive Quality, Compliance, and Resilience Model

The proposed model is a conceptual decision-support framework, not a validated regulatory algorithm. It combines supplier-performance records and risk signals to help quality, procurement, and regulatory teams identify concerns early and prioritise proportionate action. It complements rather than replaces supplier qualification, audits, quality-system controls, and professional judgement, reflecting the linked roles of risk assessment and mitigation in supply-chain disruption management (Kleindorfer & Saad, 2005; Tang, 2006).

5.1 Predictive Quality Risk

Predictive quality risk estimates whether future supplier performance may contribute to non-conforming material, component failure, unstable output, or recurrent quality events. Inputs may include incoming-inspection results, supplier deviations, non-conformance reports, lot-release records, complaint investigations where supplier involvement is confirmed, CAPA records, change-control histories, and lot-level traceability data. Analysing these data as time series and event histories, rather than isolated incidents, enables the system to detect increasing or recurrent failures and their concentration in particular component families.

Trend analysis, statistical process-control measures, anomaly detection, and supervised machine learning can be used where historical data are sufficiently complete and accurately labelled. Rising rejection rates, repeated deviations for the same component, prolonged CAPA closure, or unusual shifts in test results may be used as early-warning features. The model should prioritise a supplier or component for expert review rather than interpret every signal as evidence of failure. This is consistent with Wagner and Bode's (2008) finding that supply-side risks are negatively associated with supply-chain performance.

Quality drift is a sustained movement away from an established performance baseline. It may appear as widening variation, gradual changes in defect patterns, or repeated low-severity deviations despite individual batches meeting acceptance limits. Alerts should assess direction, persistence, severity, and recurrence, then be validated by quality specialists because changed inspection intensity, data-entry errors, or approved process changes can create misleading patterns.

5.2 Predictive Compliance Risk

Predictive compliance risk estimates the likelihood that a supplier will create documentation, audit, change-control, or quality-agreement deficiencies that compromise oversight of purchased products and services. Relevant indicators include overdue CAPAs, repeated audit observations, incomplete qualification files, delayed responses to findings, missing certificates or traceability evidence, unapproved process changes, and late notification of changes to materials, sites, test methods, or subcontractors.

The system can assess the completeness, timeliness, severity, and recurrence of these records to produce a compliance-risk profile. Natural-language processing may help sort audit narratives, deviations, and CAPA descriptions into themes, but qualified personnel must determine regulatory significance. An AI alert is therefore a prioritisation tool, not a compliance conclusion. Pettit et al. (2010) conceptualise resilience as a balance between vulnerabilities and capabilities; here, documentation governance, prompt corrective action, and transparent supplier communication are capabilities that reduce vulnerability. This aligns with Christopher and Peck's (2004) emphasis on risk-management culture and resilient supply-chain design.

5.3 Predictive Supply Chain Resilience

Predictive resilience evaluates whether the supply network can absorb disruption, adapt sourcing or production arrangements, and restore dependable supply. Relevant indicators include component criticality, single-source dependency, geographic concentration, lead-time variability, inventory coverage, capacity constraints, availability of qualified alternatives, and the estimated time needed to approve a replacement source. Verified logistics, financial, geopolitical, and environmental signals can complement these internal indicators.

The system can support scenario analysis by estimating the consequences of a supplier outage for inventory, production schedules, service continuity, and recovery priorities. Ivanov and Dolgui (2021) describe digital supply-chain twins as models that represent supply-network states and combine model-based with data-driven analysis for disruption management. This supports assessment of potential mitigation actions, such as alternate-source qualification, risk-based inventory buffers, allocation rules, and contingency arrangements. Norrman and Jansson's (2004) Ericsson case likewise shows the value of combining supplier collaboration with formal risk-management processes following a major sub-supplier disruption.

5.4 Supplier Risk Scoring Model

The proposed Overall Supplier Risk Score (OSRS) is:

$$OSRS = 0.30Q + 0.25C + 0.20D + 0.15R + 0.10E$$

Q denotes quality risk, C compliance risk, D delivery risk, R resilience risk, and E external-disruption exposure. Each dimension is normalised to 0-100, with higher values indicating greater risk. The weights are proposed for this paper, not claimed as an industry standard. Quality and compliance are weighted most heavily because supplied material must remain conforming and adequately controlled. In practical use, variables, weights, and thresholds should be calibrated against historical performance, component criticality, and approved organisational risk criteria.

For illustration, scores below 30 are low, 30-49 moderate, 50-69 high, and 70-100 critical. These management categories guide review and mitigation, not automatic supplier disqualification. They reflect the principle that preparedness and mitigation should precede disruption (Christopher & Peck, 2004).

5.5 Scenario-Based Illustration

Table 4 uses fictional data solely to demonstrate the model. Supplier A is suitable for routine monitoring. Supplier B requires intensified incoming inspection, CAPA review, and a delivery-recovery plan. Supplier C requires urgent contingency assessment because high compliance, resilience, and external-exposure scores occur together. Supplier D is appropriate for structured supplier development and closer trend monitoring. The scores are neither observed supplier results nor validated industry benchmarks.

Table 4 Hypothetical Supplier Risk Scorecard for Medical Device Manufacturers

Supplier	Quality Risk Score	Compliance Risk Score	Delivery Risk Score	Resilience Risk Score	External Disruption Score	Overall Risk Rating	Recommended Action
Supplier A	18	20	24	22	15	Low (20.0)	Routine monitoring
Supplier B	58	46	64	45	30	High (51.5)	CAPA review, intensified receiving inspection, recovery plan
Supplier C	72	78	55	70	80	Critical (70.6)	Contingency assessment and alternative-source review
Supplier D	38	35	42	40	28	Moderate (37.4)	Supplier development and trend monitoring

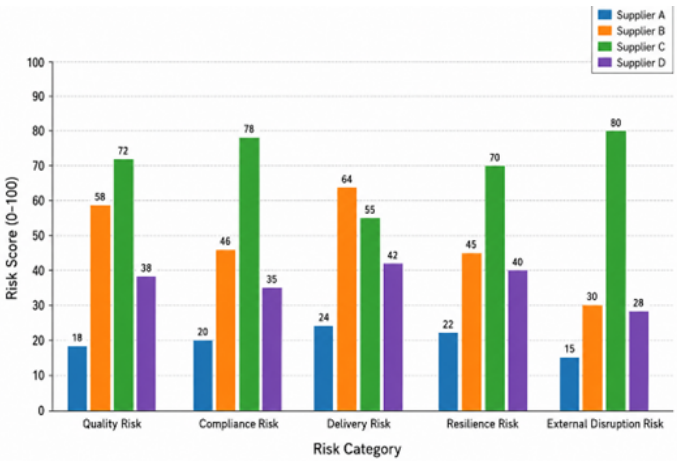

Figure 3 *Comparative Supplier Risk Scores Across Five Risk Categories*

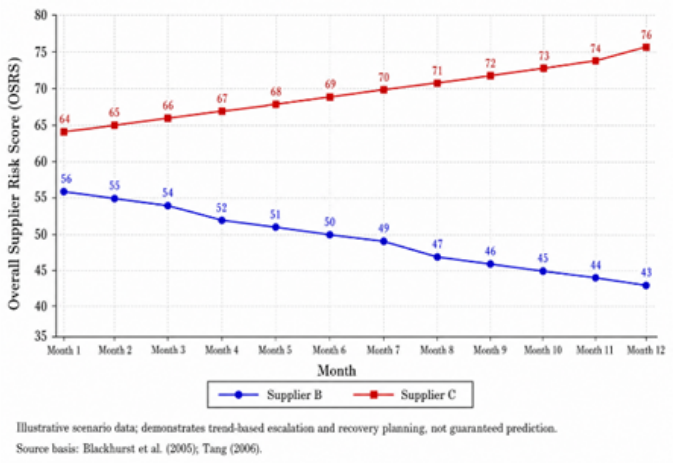

Figure 4 *Illustrative Predicted Overall Risk Trend Over 12 Months*

6. Discussion

6.1 Contribution to Medical Device Supplier Risk Management

The proposed cognitive supplier risk management framework contributes to medical device supply chain management by shifting supplier oversight from a reactive compliance function to a predictive, intelligence-driven process. Traditional supplier management often depends on periodic audits, historical defect reports, delayed corrective actions, and manual supplier scorecards. While these methods remain important, they may fail to detect early signs of supplier instability, quality drift, documentation gaps, or emerging disruption risks. The proposed framework improves supplier visibility by integrating quality, regulatory, operational, logistics, and external risk data into a unified analytical environment. This allows manufacturers to monitor supplier performance more continuously and identify weak signals before they develop into serious quality or compliance failures.

In relation to quality prediction, the framework supports early detection of supplier-related non-conformance, process variation, recurring defects, and component reliability concerns. By applying artificial intelligence to supplier quality records, audit findings, complaint trends, and corrective action histories, manufacturers can move beyond retrospective defect analysis toward predictive quality assurance. This is particularly important in the medical device sector, where supplier failures may directly affect device safety, clinical performance, and patient outcomes. The framework also strengthens compliance readiness by supporting traceable, auditable, and evidence-based supplier monitoring. Since medical device regulation requires strong documentation, supplier qualification, risk control, and post-market accountability, predictive supplier intelligence can help firms identify compliance weaknesses before regulatory inspection or market disruption occurs (Maisel, 2004; Kramer et al., 2020).

The framework also improves supply chain resilience by helping organizations identify vulnerable suppliers, evaluate alternative sourcing options, and prioritize mitigation actions. Instead of treating resilience only as a recovery activity after disruption, the framework positions resilience as an anticipatory capability supported by AI-enabled forecasting and decision

support. This makes supplier risk management more dynamic, especially for manufacturers operating across global and highly regulated supply networks.

6.2 Theoretical Contribution

The study contributes theoretically by connecting four major knowledge areas: supplier risk theory, supply chain resilience theory, AI-based decision support, and medical device regulatory governance. Supplier risk theory explains how uncertainty in supplier capability, reliability, delivery, quality, and financial stability can create operational and strategic exposure for buying firms. The proposed framework extends this view by showing that supplier risk in the medical device industry is not only a commercial or operational concern, but also a patient safety and regulatory compliance issue.

The study also builds on resilience theory by linking risk anticipation, adaptive capacity, visibility, and recovery planning to cognitive analytics. Resilience is not treated merely as the ability to recover from disruption, but as the ability to predict, prepare, respond, and learn. AI-based decision support adds another theoretical layer by explaining how machine learning, anomaly detection, natural language processing, and risk scoring can enhance managerial interpretation of complex supplier data. However, the framework does not assume that AI should replace human judgement. Instead, it positions AI as an assistive intelligence layer that supports risk interpretation, prioritization, and governance. This aligns with broader arguments that AI in healthcare and medical technology must be designed with clinical, organizational, ethical, and regulatory oversight in mind (Kelly et al., 2019; Wiens et al., 2019; Reddy et al., 2020).

Finally, the framework contributes to regulatory governance theory by emphasizing that AI-enabled supplier risk systems must remain explainable, documented, and auditable. This is consistent with concerns raised about AI-based medical technologies, where transparency, validation, accountability, and system-level regulation are required to prevent unsafe or poorly governed implementation (Gerke et al., 2020; Pesapane et al., 2018).

6.3 Practical Implications

Practically, the proposed framework can support several stakeholders within medical device manufacturing. For manufacturers, it provides a structured method for identifying high-risk suppliers and improving continuity of supply. For quality managers, it supports earlier detection of non-conformance trends, supplier corrective action delays, audit weaknesses, and recurring defect patterns. This can improve supplier quality management and reduce the likelihood of product holds, recalls, or regulatory findings.

For procurement teams, the framework can improve supplier selection, segmentation, and contract monitoring by incorporating predictive risk indicators alongside price and delivery performance. For regulatory affairs teams, the system can strengthen inspection readiness by ensuring that supplier documentation, quality agreements, corrective actions, and risk controls are continuously monitored. For supply chain leaders, the framework provides a decision-support tool for resilience planning, supplier diversification, inventory prioritization, and disruption response. The practical value of the system lies in its ability to connect quality, compliance, and supply continuity into one integrated supplier intelligence model.

6.4 Regulatory and Ethical Implications

The use of AI in supplier risk management creates important regulatory and ethical responsibilities. Since supplier decisions can affect device quality and patient safety, AI-generated risk scores must be explainable, auditable, validated, and subject to human review. A supplier should not be penalized, removed, or downgraded solely because of an opaque algorithmic output. Decision-makers must understand which data points influenced a risk score and whether the model's conclusion is supported by reliable evidence.

The framework therefore requires strong governance controls, including model validation, data traceability, performance monitoring, access control, and documented human oversight. These requirements are consistent with wider debates on AI in medical devices and healthcare, where poor validation, weak transparency, biased data, and unclear accountability can undermine trust and safety (Benjamens et al., 2020; Gerke et al., 2020; Reddy et al., 2020). Ethical implementation also requires fairness in supplier evaluation, especially when smaller suppliers may have less complete digital records than larger firms.

6.5 Implementation Challenges

Despite its potential, implementation may be difficult. Data fragmentation remains a major barrier because supplier information is often distributed across enterprise resource planning systems, quality management systems, audit files, regulatory databases, spreadsheets, emails, and supplier portals. Poor data quality can also weaken AI performance, especially when records are incomplete, inconsistent, outdated, or manually entered.

Algorithmic bias is another concern. If historical supplier evaluations contain biased assumptions or incomplete evidence, AI models may reproduce those patterns. Limited interoperability between quality, regulatory, procurement, and logistics systems can also prevent real-time supplier visibility. Model validation presents an additional challenge because medical device manufacturers must demonstrate that AI outputs are reliable, explainable, and appropriate for regulated decision-making. Supplier resistance may also occur if firms view the system as punitive surveillance rather than collaborative risk improvement. Finally, regulatory uncertainty remains a concern because AI-based supplier risk tools sit at the intersection of quality management, supply chain governance, and medical device regulation. For this reason, implementation should be gradual, transparent, validated, and supported by clear human accountability.

7. Conclusion and Future Research Directions

7.1 Conclusion

Medical device supply chains operate in a setting where supplier performance is directly connected to product quality, regulatory compliance, patient safety, and production continuity. This paper has argued that conventional supplier risk management remains necessary but is increasingly insufficient when it depends mainly on periodic audits and retrospective scorecards. These controls often reveal problems only after a quality deviation, documentation gap, delivery failure, or supply interruption has affected operations. A cognitive supplier risk management system provides a more proactive alternative by integrating internal and external data, identifying weak signals, forecasting emerging threats, and

translating analytical outputs into practical actions.

The proposed framework treats artificial intelligence as an enabling capability rather than a replacement for professional judgment. Its value lies in combining predictive quality analytics, compliance intelligence, and resilience planning within one decision-support environment. It can help manufacturers identify deteriorating supplier risk profiles before they lead to non-conforming components, production delays, regulatory exposure, or patient harm. The framework consequently supports a system-level approach to supplier risk, connecting operational performance with quality assurance and regulatory accountability. It also reflects the transition toward data-driven, digitally connected supply chains in which timely intelligence supports preparedness, response, and recovery (Baryannis et al., 2019; Ivanov & Dolgui, 2021).

7.2 Key Findings

Several findings emerge from the analysis. First, supplier risk in medical device supply chains is multidimensional. It extends beyond price, capacity, and delivery to include component quality, traceability, documentation accuracy, audit findings, corrective-action performance, cybersecurity, and disruption vulnerability. Risk should therefore be assessed across operational, strategic, and environmental dimensions rather than through a narrow supplier scorecard (Ho et al., 2015; Wang et al., 2016).

Second, traditional supplier monitoring is commonly reactive. Audits, non-conformance reviews, and performance reports are important safeguards, yet they frequently rely on lagging indicators. By the time declining quality, late corrective actions, or recurring delivery variability are visible, the underlying problem may already be difficult or costly to contain. Cognitive systems can address this weakness through continuous data integration, anomaly detection, predictive modelling, and dynamic risk prioritisation. These methods can detect patterns that are difficult to identify through fragmented manual review and provide earlier warnings of supplier deterioration (Toorajipour et al., 2021; Baryannis et al., 2019).

Third, AI can support earlier detection of quality and compliance risks. Machine-learning models may identify recurring defects, rising deviation rates, overdue corrective actions, or unusual documentation changes. Natural language processing can extract evidence from audit reports, supplier communications, and quality-event narratives. The principal benefit is not simply faster analysis, but the capacity to connect dispersed signals that collectively indicate increased risk.

Fourth, cognitive systems can improve resilience by supporting predictive intelligence and scenario-informed decisions. In the proposed model, resilience is not treated solely as post-disruption recovery. It is an ongoing capability supported by supplier visibility, alternative sourcing evaluation, inventory planning, and disruption simulation. Digital supply chain twins can help managers assess the likely effects of a supplier failure and compare mitigation options before a disruption occurs (Ivanov & Dolgui, 2021). This view aligns with resilience scholarship emphasizing anticipation, adaptability, collaboration, and recovery capacity (Hohenstein et al., 2015).

Finally, human governance remains indispensable. AI-generated risk scores and recommendations should support, not replace, expert decisions. Quality, procurement, regulatory, and supply chain leaders must validate outputs, investigate high-risk signals, approve mitigation actions, and ensure that the system is transparent, auditable, and aligned with organizational and regulatory requirements.

7.3 Limitations

This paper is conceptual and framework-based. It develops an integrated model from existing scholarship rather than testing predictive performance with a real medical device manufacturer dataset. The proposed relationships among risk indicators, AI techniques, and management outcomes therefore require empirical validation. It does not assign final weights to risk variables, compare specific algorithms, or quantify implementation costs. Deployment may also be constrained by data availability, interoperability, confidentiality, and data quality. It should consequently be interpreted as a strategic design for future implementation rather than a validated operational tool.

7.4 Future Research

Future research should test the framework using real supplier performance data from medical device manufacturers. Relevant datasets could include audit findings, non-conformance records, corrective-action histories, incoming inspection results, delivery performance, regulatory observations, and quality-event data. Longitudinal studies are especially important because they can determine whether early warning indicators reliably predict later quality failures, compliance deficiencies, or supply disruptions.

Researchers should compare supervised learning, anomaly detection, natural language processing, knowledge graphs, and hybrid rule-based models for predictive accuracy and explainability. Further work should examine whether digital supply chain twins improve supplier substitution, inventory buffering, and disruption-response planning. Multi-case research across device categories and regulatory jurisdictions would show how the framework should be adapted for different organizations and high-risk technologies. Such studies would move the framework toward an evidence-based capability for safer, compliant, and resilient medical device supply chains.

References

1. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. 10.1108/09574090410700275
2. Kusiak, A. (2018). Smart manufacturing. International journal of production Research, 56(1-2), 508-517. 10.1080/00207543.2017.1351644
3. Ali, A., Mahfouz, A., & Arisha, A. (2017). Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review. Supply chain management: an international journal, 22(1), 16-39. 10.1108/scm-06-2016-0197
4. Baryannis, G., Dani, S., & Antoniou, G. (2019). Predictive analytics and artificial intelligence in supply chain management: Review and implications for the future. Computers & Industrial Engineering, 137(106024). 10.1007/978-3-030-03813-7_4
5. Benjamens, S., Dhunnoo, P., & Meskó, B. (2020). The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database. NPJ digital

medicine, 3(1), 118. 10.1038/s41746-020-00324-0

6. Blackhurst*, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. International journal of production research, 43(19), 4067-4081. 10.1080/00207540500151549

7. Gerke, S., Babic, B., Evgeniou, T., & Cohen, I. G. (2020). The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. NPJ digital medicine, 3(1), 53. 10.1038/s41746-020-0262-2

8. Hazen, B. T., Boone, C. A., Ezell, J. D., & Jones-Farmer, L. A. (2014). Data quality for data science, predictive analytics, and big data in supply chain management: An introduction to the problem and suggestions for research and applications. International journal of production economics, 154, 72-80. 10.1016/j.ijpe.2014.04.018

9. Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: a literature review. International journal of production research, 53(16), 5031-5069. 10.1080/00207543.2015.1030467

10. Hohenstein, N. O., Feisel, E., Hartmann, E., & Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: a systematic review and paths for further investigation. International journal of physical distribution & logistics management, 45(1-2), 90-117. 10.1108/ijpdlm-05-2013-0128

11. Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control, 32(9), 775-788. 10.1080/09537287.2020.1768450

12. Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management. International journal of operations & production management, 37(1), 10-36. 10.1108/ijopm-02-2015-0078

13. Kelly, C. J., Karthikesalingam, A., Suleyman, M., Corrado, G., & King, D. (2019). Key challenges for delivering clinical impact with artificial intelligence. BMC medicine, 17(1), 195. 10.1186/s12916-019-1426-2

14. Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. Production and operations management, 14(1), 53-68. 10.1111/j.1937-5956.2005.tb00009.x

15. Kramer, D. B., Xu, S., & Kesselheim, A. S. (2020). Regulation of medical devices in the United States and European Union. In The ethical challenges of emerging medical technologies (pp. 41-48). Routledge. 10.4324/9781003074984-3

16. Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing letters, 3, 18-23. 10.1016/j.mfglet.2014.12.001

17. Maisel, W. H. (2004). Medical device regulation: an introduction for the practicing physician. Annals of internal medicine, 140(4), 296-302. 10.7326/0003-4819-140-4-200402170-00012

18. Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. Journal of business logistics, 29(1), 133-155. 10.1002/j.2158-1592.2008.tb00072.x

19. Min, H. (2010). Artificial intelligence in supply chain management: theory and applications. International Journal of Logistics: Research and Applications, 13(1), 13-39. 10.1080/13675560902736537

20. Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. International journal of physical distribution & logistics management, 34(5), 434-456. 10.1108/09600030410545463

21. Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights into imaging, 9(5), 745-753. 10.1007/s13244-018-0645-y

22. Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. Journal of business logistics, 31(1), 1-21. 10.1002/j.2158-1592.2010.tb00125.x

23. Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. Journal of the American medical informatics association, 27(3), 491-497. 10.1093/jamia/ocz192

24. Tang, C. S. (2006). Perspectives in supply chain risk management. International journal of production economics, 103(2), 451-488. 10.1016/j.ijpe.2005.12.006

25. Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. Journal of business research, 122, 502-517. 10.1016/j.jbusres.2020.09.009

26. Wagner, S. M., & Bode, C. (2008). An empirical examination of supply chain performance along several dimensions of risk. Journal of business logistics, 29(1), 307-325. 10.1002/j.2158-1592.2008.tb00081.x

27. Waller, M. A., & Fawcett, S. E. (2013). Data science, predictive analytics, and big data: a revolution that will transform supply chain design and management. Journal of Business logistics, 34(2), 77-84. 10.1111/jbl.12010

28. Wang, G., Gunasekaran, A., Ngai, E. W., & Papadopoulos, T. (2016). Big data analytics in logistics and supply chain management: Certain investigations for research and applications. International journal of production economics, 176, 98-110. 10.1016/j.ijpe.2016.03.014

29. Wiens, J., Saria, S., Sendak, M., Ghassemi, M., Liu, V. X., Doshi-Velez, F., ... & Goldenberg, A. (2019). Do no harm: a roadmap for responsible machine learning for health

care. Nature medicine, 25(9), 1337-1340. 10.1038/s41591-019-0548-6

30. Zsidisin, G. A. (2003). A grounded definition of supply risk. Journal of purchasing and supply management, 9(5-6), 217-224. 10.1016/j.pursup.2003.07.002