DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Bahrami Far, J., Dehghan Dehnavi, H., Sadeghian, A., & Rabbani, M. (2026). Agile Risk Management Model Based on the Internet of Things Using a System Dynamics Approach. *Digital Transformation and Administration Innovation,* 4(4), 1-20.

Received date: 2025-12-16 Revised date: 2026-04-28 Accepted date: 2026-05-05 Published date: 2026-07-01

Agile Risk Management Model Based on the Internet of Things Using a System Dynamics Approach

Jaber Bahrami Far [1], Hasan Dehghan Dehnavi [1]*, Abolfazl Sadeghian [1], Mojde Rabbani [1]

1. Department of Industrial Management, Ya.C., Islamic Azad University, Yazd, Iran

*Correspondence: Denavi2000@iau.ac.ir

Abstract

The present study aimed to design and present an agile risk management model based on the Internet of Things (IoT) using a system dynamics approach in order to improve organizational agility, resilience, and decision-making capability in complex and dynamic environments. Methods and Materials: This applied and descriptive-correlational study employed a mixed-methods approach combining qualitative and quantitative techniques. Data were collected through library research, structured interviews, and standard questionnaires. In the qualitative phase, 15 experts from Iran Khodro Company in Tehran participated until theoretical saturation was achieved. The statistical population in the quantitative phase consisted of industrial experts and specialists from large companies in Kerman Province selected through simple random sampling. Data validity and reliability were confirmed using content validity, Cronbach's alpha, and the qualitative trustworthiness criteria of Guba and Lincoln. Data analysis was conducted using SPSS, SmartPLS, and Vensim software. The Delphi technique, Friedman test, Kendall's coefficient, and system dynamics modeling including Causal Loop Diagram (CLD) and Stock and Flow Diagram (SFD) were applied to analyze relationships among variables and simulate system behavior over time. Findings: Inferential findings demonstrated that all identified indicators of agile IoT-based risk management were statistically confirmed by experts in both Delphi rounds ($p < 0.05$). Kendall's coefficient increased from 0.703 in the first round to 0.912 in the second round, indicating strong consensus among experts. The most significant components included rapid identification of IoT-related risks, continuous monitoring of IoT service quality, integration of risks into agile development cycles, and rapid response to unexpected events. System dynamics simulation revealed that increased risk knowledge enhanced organizational resilience and agility through reinforcing feedback loops. Sensitivity and scenario analyses showed that increasing the rate of real-time risk data collection significantly improved resilience capacity and long-term system stability, whereas weak infrastructure and delayed responses reduced system adaptability. The findings further indicated that leverage points such as accumulated risk knowledge and resilience capacity had the greatest impact on improving overall system performance. Conclusion: The results confirmed that agile risk management in IoT ecosystems requires a systemic, dynamic, and integrated perspective that simultaneously addresses security, resilience, organizational agility, infrastructure quality, and rapid decision-making. The proposed model demonstrated that balancing reinforcing and balancing feedback loops is essential for sustaining organizational performance under uncertain conditions. The framework can serve as a practical and strategic reference for managers and researchers in digital supply chains and IoT-based project management environments.

Keywords: Agile Risk Management, Internet of Things, System Dynamics, Organizational Agility, Digital Supply Chain, Resilience, IoT Security, Risk Prediction

1. Introduction

The rapid expansion of digital technologies, intelligent infrastructures, and interconnected systems has fundamentally transformed organizational environments and operational processes in recent years. Among these emerging technologies, the Internet of Things (IoT) has become one of the most influential drivers of digital transformation across industries, supply chains, industrial systems, healthcare, logistics, and smart manufacturing. IoT ecosystems enable organizations to collect, process, and exchange massive volumes of real-time data through interconnected sensors, smart devices, and communication infrastructures. While these technologies improve operational efficiency, automation, responsiveness, and decision-making capabilities, they simultaneously increase the complexity, uncertainty, and vulnerability of organizational systems (Abernikhina, 2025; Abernikhina et al., 2025). As a result, organizations increasingly face multidimensional risks associated with cybersecurity threats, data privacy violations, infrastructure instability, system failures, communication disruptions, and operational uncertainty. Traditional risk management approaches, which were originally designed for relatively stable and linear organizational environments, are no longer sufficient for addressing the dynamic and nonlinear risks emerging in IoT-based ecosystems (Acebes, Curto, et al., 2024; Acebes, Gonzalez-Varona, et al., 2024).

Risk management has evolved significantly from conventional probabilistic approaches toward integrated, dynamic, and digitally oriented models. Contemporary theories emphasize adaptive, data-driven, and resilient approaches capable of responding to rapidly changing environments and interconnected organizational structures (Abernikhina et al., 2025). The emergence of digital-ESG-oriented risk management models has further reinforced the need for integrating technological intelligence, sustainability, cybersecurity, and organizational agility within modern risk management systems (Abernikhina, 2025). In IoT environments, risk management is no longer limited to identifying isolated technical threats; instead, it requires continuous monitoring, predictive analytics, rapid response mechanisms, and dynamic adaptation to evolving risks. These requirements have intensified the importance of agile risk management approaches capable of integrating real-time information flows, intelligent decision-making, and organizational learning mechanisms (Affia et al., 2023; Al-Dosari & Fetais, 2023).

Agile methodologies were initially developed within software engineering and project management to improve flexibility, iterative development, rapid response, and customer-oriented adaptation. Over time, agile principles have expanded beyond software development and have become relevant in broader organizational and technological contexts, particularly in highly uncertain and rapidly changing environments (Azari & Javadani Gandomani, 2018). Agile risk management emphasizes continuous identification, assessment, monitoring, and mitigation of risks throughout the operational lifecycle rather than relying on static and predefined risk-control procedures. This adaptive orientation makes agile approaches especially suitable for IoT ecosystems, where risks evolve continuously due to changes in network structures, device interactions, cyber threats, and environmental uncertainties (Afshari & Gandomani, 2022; Feyzi et al., 2020). Agile systems are capable of supporting iterative learning, decentralized decision-making, collaborative problem-solving, and rapid feedback loops, all of which are critical for maintaining resilience in digital infrastructures.

The integration of IoT technologies with agile management principles creates substantial opportunities for improving organizational responsiveness and risk mitigation. Real-time sensor data, machine learning algorithms, predictive analytics, and intelligent monitoring systems allow organizations to identify anomalies, detect vulnerabilities, and respond rapidly to disruptions before they escalate into major operational crises (Rahimi Kalvar & Ghasemi Hamadani, 2023; Rezaeian & Mollahosseini, 2017). Artificial intelligence-based risk management systems have demonstrated considerable potential for improving supply chain agility, predictive maintenance, operational continuity, and adaptive decision-making in complex digital ecosystems (Rahimi Kalvar & Ghasemi Hamadani, 2023). Similarly, intelligent agents and automated detection mechanisms have been proposed as effective tools for identifying hidden risks, improving cybersecurity, and enhancing the efficiency of agile software development projects (Rezaeian & Mollahosseini, 2017). These technological capabilities are particularly important in IoT environments because interconnected devices generate large-scale and high-velocity data streams that cannot be effectively managed through manual or static approaches.

Despite these opportunities, IoT ecosystems introduce new categories of risk that challenge traditional management structures. One of the most critical challenges involves cybersecurity vulnerabilities. IoT devices often operate through

heterogeneous networks with varying security standards, making them vulnerable to cyberattacks, unauthorized access, data manipulation, and system disruption (Abu Talib et al., 2022; Al-Hamar et al., 2021). Advanced persistent threats, phishing attacks, social engineering attacks, and malicious beaconing activities represent major concerns within connected industrial and organizational systems (Abu Talib et al., 2022; Aldawood & Skinner, 2020). Security risks become even more complicated when organizations rely on cloud infrastructures, distributed communication systems, and multi-supplier ecosystems. Consequently, modern IoT risk management requires integrated cybersecurity frameworks capable of balancing security protection, service quality, operational agility, and infrastructure resilience (Affia et al., 2023; Al-Dosari et al., 2023).

The adoption of IoT technologies within supply chains and industrial operations has also highlighted the importance of system integration and organizational coordination. Research on digital supply chains has shown that successful IoT implementation depends heavily on integration capability, communication infrastructure, data transparency, and collaborative agility among stakeholders (Pourbagher et al., 2023). IoT systems involve continuous interaction among hardware devices, software applications, cloud platforms, sensors, communication protocols, and human operators. This interconnectedness creates highly interdependent environments in which local disruptions may rapidly propagate across the network and generate systemic consequences. Therefore, organizations require holistic and dynamic risk management models capable of analyzing network effects, system dependencies, and nonlinear feedback structures (Al-Dosari & Fetais, 2023). Traditional linear analytical tools are often insufficient for modeling such environments because they cannot adequately capture delayed effects, reinforcing feedback loops, adaptive responses, and dynamic interactions among organizational components.

In response to these limitations, system dynamics has emerged as an effective methodological approach for analyzing complex systems characterized by feedback loops, delays, accumulations, and nonlinear interactions. System dynamics provides researchers and decision-makers with tools for understanding long-term system behavior, simulating alternative scenarios, and identifying leverage points that significantly influence organizational performance (Abdel-Latif, 2023). Through causal loop diagrams and stock-and-flow modeling, system dynamics enables organizations to analyze how changes in one component influence the broader system over time. This capability is particularly valuable for IoT risk management because digital ecosystems involve continuous interactions among cybersecurity investment, quality of service, organizational agility, resilience capacity, data quality, and infrastructure performance (Ahmad & Sarjoughian, 2023). Dynamic simulation approaches allow organizations to test different risk mitigation policies, evaluate the long-term consequences of strategic decisions, and optimize resource allocation under uncertain conditions (Al-Dosari & Fetais, 2023).

Several studies have attempted to improve agile risk management within software development and IoT contexts. Research on Scrum and Extreme Programming methodologies has emphasized the importance of integrating risk identification and mitigation mechanisms directly into agile development cycles (Azari & Javadani Gandomani, 2018). Process-oriented agile risk management frameworks have also been proposed to improve responsiveness, iterative monitoring, and team-based collaboration in software projects (Feyzi et al., 2020). Other studies have explored hybrid agile methodologies and integrated risk management models capable of combining flexibility with systematic control mechanisms (Afshari & Gandomani, 2022). These studies collectively demonstrate that agile methodologies can significantly improve risk visibility, communication efficiency, and organizational adaptability. However, most existing models focus primarily on software development environments and do not adequately address the broader technological and infrastructural complexities associated with IoT ecosystems.

In the context of IoT, previous studies have primarily concentrated on adoption factors, cybersecurity frameworks, intelligent detection systems, and communication infrastructures (Affia et al., 2023; Pourbagher et al., 2023). While these contributions are valuable, they often examine isolated dimensions of IoT risk management rather than providing a comprehensive and integrated framework capable of capturing the dynamic interactions among agility, resilience, cybersecurity, infrastructure quality, and organizational adaptation. Similarly, studies on cloud-based knowledge management systems emphasize the importance of organizational culture, trust, human factors, and integration capability in achieving successful digital transformation (Khadivar & Dortaj, 2021). These findings indicate that technological advancement alone is insufficient unless accompanied by adaptive organizational structures and collaborative learning processes.

The growing complexity of industrial systems, digital supply chains, and interconnected infrastructures further reinforces the need for dynamic and adaptive risk management approaches. Simulation-based methodologies and quantitative risk analysis tools have become increasingly important for improving decision-making quality and understanding uncertainty in complex organizational systems (Acebes, Curto, et al., 2024; Acebes, Gonzalez-Varona, et al., 2024). Monte Carlo simulation, system dynamics modeling, and scenario analysis provide valuable mechanisms for evaluating risk propagation, infrastructure vulnerability, resilience capacity, and strategic trade-offs. Moreover, recent advances in simulation modeling environments have enabled the development of integrated frameworks capable of combining software architecture modeling, dynamic simulation, and risk analysis within a unified analytical environment (Ahmad & Sarjoughian, 2023). These developments create significant opportunities for designing more effective agile IoT-based risk management systems.

Nevertheless, important research gaps remain unresolved. Existing studies have not sufficiently integrated agile management principles, IoT infrastructure dynamics, cybersecurity requirements, organizational resilience, and system dynamics modeling into a unified analytical framework. Many current models either focus on static risk assessment, isolated technical threats, or software-oriented agile processes without considering the systemic and feedback-driven nature of IoT ecosystems (Kazemi & Salajegheh, 2017; Mousaei et al., 2015). Furthermore, previous research has rarely combined qualitative coding approaches, Delphi consensus techniques, and system dynamics simulation within a single comprehensive model capable of supporting strategic and operational decision-making. This gap is particularly important because IoT ecosystems require continuous adaptation, real-time monitoring, rapid response capability, and integrated coordination among organizational, technological, and infrastructural dimensions.

Given these challenges, there is a clear need for a comprehensive framework that combines agile risk management principles with IoT technologies and system dynamics modeling. Such a framework should be capable of identifying critical risk factors, analyzing dynamic relationships among system components, simulating long-term organizational behavior, and supporting strategic decision-making under uncertainty. In addition, the framework should integrate cybersecurity management, resilience enhancement, quality-of-service monitoring, DevOps integration, infrastructure coordination, and organizational agility within a unified conceptual structure. Addressing these requirements can significantly improve the capacity of organizations to manage digital risks, maintain operational continuity, and adapt effectively to rapidly changing technological environments.

Therefore, the present study aims to design and present an agile risk management model based on the Internet of Things using a system dynamics approach in order to identify key risk-management components, analyze their dynamic interactions, and improve organizational agility, resilience, and decision-making capability in complex digital ecosystems.

2. Methods and Materials

The present study was conducted using a mixed-methods approach with an applied objective and a descriptive-correlational design. The research sought to develop an agile risk management model based on the Internet of Things (IoT) using a system dynamics approach. The study combined qualitative and quantitative procedures in order to identify the main dimensions of agile IoT-based risk management, validate the extracted indicators, and simulate the dynamic interactions among the components of the proposed model. In the qualitative phase, data were collected through an extensive review of domestic and international literature, semi-structured and in-depth interviews, and expert evaluations. The qualitative population consisted of specialists, managers, and experts working in industrial organizations with experience in agile management, digital supply chains, IoT infrastructure, and risk management systems. Fifteen experts from Iran Khodro Company in Tehran participated in the interview phase, and theoretical saturation was achieved after completing the interviews. The participants were selected purposively based on their professional expertise, managerial experience, and familiarity with agile systems and IoT technologies.

In the quantitative phase, the statistical population included experts and specialists from large industrial companies located in Kerman Province who were directly or indirectly involved in digital transformation, IoT implementation, project management, or organizational risk management activities. Because the exact number of experts was not clearly identifiable, simple random sampling was employed to select the participants. Data collection in the quantitative section relied on a standardized questionnaire developed based on the findings of the qualitative phase and previous theoretical studies. The study focused on evaluating the relationships among the dimensions of agile risk management, including risk identification,

cybersecurity management, organizational agility, infrastructure resilience, data quality, rapid response capability, and DevOps integration. The mixed-methods design enabled the researchers to integrate qualitative insights with quantitative validation and dynamic simulation in order to produce a comprehensive and operational model for agile risk management in IoT environments.

Data collection in the qualitative phase was carried out using semi-structured and in-depth interviews as the primary instrument. The interviews were designed to explore experts' perceptions regarding the challenges, requirements, and critical success factors of agile risk management in IoT-based systems. The interview protocol included questions related to risk identification, cybersecurity threats, resilience mechanisms, organizational agility, real-time monitoring, DevOps integration, and supply chain coordination. The interviews allowed direct interaction with participants and provided opportunities for deeper exploration of their experiences, attitudes, and interpretations regarding complex organizational and technological issues. In addition to interviews, library-based methods such as reviewing scientific articles, conference papers, dissertations, and electronic databases were employed to collect theoretical foundations and identify initial indicators of the model.

In the quantitative phase, a standardized questionnaire was utilized to validate the conceptual model and measure the identified constructs. The questionnaire consisted of 40 indicators related to agile IoT-based risk management dimensions. These indicators included rapid identification of IoT-related risks, anomaly detection in IoT networks, real-time monitoring of service quality, cybersecurity management, dynamic access control, machine learning-based risk prediction, organizational agility, resilience capacity, and integration of DevOps tools with IoT risk management systems. The questionnaire items were designed using a five-point Likert scale ranging from very low to very high. Content validity was assessed through expert evaluation and review by university professors and industry specialists. The overall content validity coefficient of the questionnaire was reported as 0.87, indicating acceptable validity. Reliability was examined using Cronbach's alpha coefficient, which yielded a value of 0.79, demonstrating satisfactory internal consistency of the instrument. In the qualitative phase, trustworthiness was ensured based on the criteria proposed by Guba and Lincoln, including credibility, transferability, dependability, and confirmability. These criteria were achieved through prolonged engagement with participants, repeated review of interview transcripts, peer debriefing, expert validation, and systematic documentation of the research procedures.

The collected data were analyzed using both qualitative and quantitative analytical techniques. In the qualitative phase, thematic coding procedures including open coding, axial coding, and selective coding were employed to identify and categorize the dimensions and components of agile IoT-based risk management. Initially, 40 primary indicators were extracted from the literature review and expert interviews. These indicators were subsequently integrated into broader conceptual categories through comparative and interpretive analysis. The Delphi technique was applied in two rounds to achieve expert consensus regarding the importance and prioritization of the identified indicators. The Friedman test and single-sample t-test were used to evaluate the significance and ranking of the indicators, while Kendall's coefficient of concordance was calculated to measure the degree of agreement among experts.

In the quantitative phase, descriptive and inferential statistical analyses were conducted using SPSS and SmartPLS software. Correlation analysis and structural evaluation were performed to examine relationships among the constructs of the proposed model. In addition, system dynamics methodology was employed to model the nonlinear and dynamic interactions among the components of agile risk management. The causal relationships among variables were first represented through a Causal Loop Diagram (CLD), which illustrated reinforcing and balancing feedback loops within the system. Subsequently, the conceptual model was transformed into a Stock and Flow Diagram (SFD) using Vensim PLE software version 7.3.5. The simulation model included major stocks such as accumulated risk knowledge, organizational agility, resilience capacity, and security investment levels, along with related inflows, outflows, and auxiliary variables. Sensitivity analysis and scenario analysis were also conducted to evaluate the effects of changes in key parameters, such as risk data collection rates and security investment, on the long-term behavior of the system. The dynamic simulation enabled the identification of leverage points and critical variables influencing resilience, agility, and overall organizational performance in IoT ecosystems.

3. Findings and Results

The statistical population of this phase consisted of all studies conducted in the field of agile risk management based on the Internet of Things with a system dynamics approach. A systematic search was conducted in domestic and international scientific databases using diverse keywords related to agile risk management, IoT-based risk management, system dynamics, digital

supply chain risk, and dynamic simulation. Because of the novelty of the subject, 20 documents were retrieved and stored for comparative meta-synthesis analysis. The selection of cases focused on theoretically useful documents capable of contributing to the formation, testing, and development of the proposed model. Based on the literature review, expert interviews, and preliminary coding, 40 initial indicators were extracted. These indicators included rapid identification of IoT-related risks, real-time response to unexpected IoT events, integration of risk into agile development cycles, real-time risk updating based on live data, intelligent monitoring of IoT equipment, automatic anomaly detection, cyber risk management, dynamic access control, sensor-data security, scalability against high data volume, continuous quality-of-service monitoring, privacy-risk assessment, DevOps integration, and coordination among hardware, software, and network teams.

Table 1. Initial Indicators and Codes of Agile IoT-Based Risk Management

Code	Component
ARI01	Rapid identification of risks related to IoT devices
ARI02	Real-time response to unexpected IoT events
ARI03	Integration of risks into the agile development cycle
ARI04	Continuous updating of risks based on real-time data
ARI05	Intelligent monitoring of IoT equipment status
ARI06	Automatic anomaly detection in IoT networks
ARI07	Rapid recovery capability from equipment failures
ARI08	Determining risk probability based on sensor data
ARI09	Use of machine learning for risk prediction
ARI10	Cyber risk management in IoT environments
ARI11	Dynamic access control for connected devices
ARI12	Ensuring security of data collected from sensors
ARI13	Reducing dependency risks related to vulnerable equipment
ARI14	Agile documentation of identified risks
ARI15	Prioritization of risks based on business delivery value
ARI16	Analysis of network effects caused by failure of an IoT node
ARI17	Reducing delay in responding to sensor disruptions
ARI18	Identification of risks caused by frequency interference
ARI19	Control of risks caused by data congestion
ARI20	System scalability against high data volume
ARI21	Assessment of IoT communication infrastructure health
ARI22	Continuous monitoring of IoT quality of service
ARI23	Risk management in device interaction with the physical environment
ARI24	Prevention of risks caused by human error in IoT settings
ARI25	Ensuring service continuity under crisis conditions
ARI26	Creating a rapid feedback loop in agile teams
ARI27	Managing rapid changes in device configuration
ARI28	Risk assessment of firmware updates
ARI29	Risk analysis of communication protocols
ARI30	Monitoring abnormal behavior of users or operators
ARI31	Transparency of risk data for the agile team
ARI32	Risk management in a multi-supplier IoT ecosystem
ARI33	Agile coordination among hardware, software, and network teams
ARI34	Reducing risks caused by battery or energy-source failure
ARI35	Assessment of consumer privacy risks
ARI36	Validation of sensor alert thresholds
ARI37	Risk analysis of relationships among connected nodes
ARI38	Adoption of flexible architecture to reduce risk
ARI39	Sensor-data quality control to prevent errors
ARI40	Integration of DevOps tools with IoT risk management

In the first Delphi round, the one-sample t-test, Friedman test, mean, standard deviation, and mean rank were calculated for the first questionnaire. The results showed that all proposed indicators were confirmed by the experts. The Friedman significance level was 0.000, indicating that the ranking of indicators was statistically meaningful and that the indicators contributed significantly to shaping the final construct.

Table 2. Results of One-Sample t-Test and Friedman Test in the First Delphi Round

Component	Mean	SD	Mean Rank	Friedman Sig.	Result
Rapid identification of IoT-related risks	3.95	1.09	52.38	0.000	Confirmed
Real-time response to unexpected IoT events	3.70	1.17	44.80		Confirmed
Integration of risks into agile development cycle	4.00	1.10	51.63		Confirmed
Continuous updating of risks based on real-time data	3.65	1.20	45.68		Confirmed
Intelligent monitoring of IoT equipment	3.80	1.26	48.25		Confirmed
Automatic anomaly detection in IoT networks	3.70	1.22	48.78		Confirmed
Rapid recovery from equipment failures	3.40	1.29	38.58		Confirmed
Risk probability estimation based on sensor data	3.45	1.14	40.48		Confirmed
Machine learning-based risk prediction	3.45	1.23	38.17		Confirmed
Cyber risk management in IoT	3.75	1.16	45.43		Confirmed
Dynamic access control	3.75	1.14	46.58		Confirmed
Sensor-data security	3.25	1.33	37.08		Confirmed
Reducing dependency on vulnerable equipment	3.20	1.25	35.55		Confirmed
Agile documentation of risks	3.80	1.15	47.40		Confirmed
Risk prioritization based on business value	3.40	1.21	40.03		Confirmed
Network-effect analysis of IoT node failure	4.00	1.07	51.63		Confirmed
Reducing response delay to sensor disruptions	3.60	1.14	43.78		Confirmed
Identification of frequency-interference risks	3.10	1.25	32.88		Confirmed
Control of data-congestion risks	3.75	1.05	45.15		Confirmed
Scalability against high data volume	3.60	1.15	40.73		Confirmed
IoT communication infrastructure health assessment	3.40	1.24	37.83		Confirmed
Continuous IoT quality-of-service monitoring	4.05	1.04	54.18		Confirmed
Risk management in physical-environment interaction	3.60	1.14	43.23		Confirmed
Prevention of human-error risks in IoT settings	3.85	1.12	47.25		Confirmed
Service continuity under crisis conditions	3.50	1.14	42.05		Confirmed
Rapid feedback loop in agile teams	3.67	1.09	9.44		Confirmed
Rapid configuration-change management	3.52	1.17	8.68		Confirmed
Firmware-update risk assessment	3.70	1.10	9.63		Confirmed
Communication-protocol risk analysis	3.52	1.20	8.75		Confirmed
Monitoring abnormal user/operator behavior	3.48	1.26	8.67		Confirmed
Risk-data transparency for agile teams	3.48	1.22	8.76		Confirmed
Multi-supplier IoT ecosystem risk management	3.38	1.29	8.22		Confirmed
Agile coordination among hardware, software, and network teams	3.36	1.14	7.76		Confirmed
Reducing battery or energy-source failure risks	3.24	1.23	7.50		Confirmed
Consumer privacy-risk assessment	3.47	1.16	8.42		Confirmed
Validation of sensor alert thresholds	3.43	1.14	8.29		Confirmed
Risk analysis of connected-node relationships	3.18	1.33	7.40		Confirmed
Flexible architecture for risk reduction	3.52	1.20	8.75		Confirmed
Sensor-data quality control	3.48	1.26	8.67		Confirmed
DevOps integration with IoT risk management	3.48	1.22	8.76		Confirmed

The first-round Delphi results indicated that experts considered all indicators important. The highest mean values belonged to continuous IoT quality-of-service monitoring, integration of risks into the agile development cycle, and network-effect analysis of IoT node failure. The lower, but still confirmed, mean values were related to frequency-interference risks, dependency on vulnerable equipment, and connected-node relationship risks. The Kendall coefficient in the first Delphi round was 0.703, with chi-square = 166.410, df = 81, and p = 0.000, showing acceptable agreement among experts.

In the second Delphi round, the same indicators were re-evaluated after feedback refinement. The findings again confirmed all indicators. The Friedman significance level remained 0.000, demonstrating that expert prioritization was statistically meaningful. Compared with the first round, the second round showed stronger convergence and higher expert consensus.

Table 3. Results of One-Sample t-Test and Friedman Test in the Second Delphi Round

Component	Mean	SD	Mean Rank	Friedman Sig.	Result
Rapid identification of IoT-related risks	4.05	1.05	55.48	0.000	Confirmed
Real-time response to unexpected IoT events	3.85	1.08	49.35		Confirmed
Integration of risks into agile development cycle	4.00	0.86	55.00		Confirmed
Continuous updating of risks based on real-time data	3.80	1.14	49.38		Confirmed
Intelligent monitoring of IoT equipment	3.45	1.15	42.75		Confirmed
Automatic anomaly detection in IoT networks	3.65	1.34	47.05		Confirmed
Rapid recovery from equipment failures	3.35	1.39	40.73		Confirmed
Risk probability estimation based on sensor data	3.10	1.19	32.23		Confirmed
Machine learning-based risk prediction	3.10	1.15	33.20		Confirmed
Cyber risk management in IoT	3.75	0.91	47.48		Confirmed
Dynamic access control	3.55	1.12	43.25		Confirmed
Sensor-data security	3.25	1.41	36.85		Confirmed
Reducing dependency on vulnerable equipment	3.10	1.36	32.67		Confirmed
Agile documentation of risks	3.75	1.20	46.65		Confirmed
Risk prioritization based on business value	3.60	1.35	43.23		Confirmed
Network-effect analysis of IoT node failure	4.05	0.86	54.88		Confirmed
Reducing response delay to sensor disruptions	3.90	1.19	51.18		Confirmed
Identification of frequency-interference risks	3.35	1.12	41.33		Confirmed
Control of data-congestion risks	4.00	0.85	52.28		Confirmed
Scalability against high data volume	3.60	1.14	44.03		Confirmed
IoT communication infrastructure health assessment	3.20	1.14	34.80		Confirmed
Continuous IoT quality-of-service monitoring	3.50	1.05	41.90		Confirmed
Risk management in physical-environment interaction	3.25	1.05	34.90		Confirmed
Prevention of human-error risks in IoT settings	3.90	0.99	49.45		Confirmed
Service continuity under crisis conditions	3.85	1.10	48.03		Confirmed
Rapid feedback loop in agile teams	3.59	1.10	9.25		Confirmed
Rapid configuration-change management	3.44	1.20	8.62		Confirmed
Firmware-update risk assessment	3.60	1.15	9.37		Confirmed
Communication-protocol risk analysis	3.48	1.23	8.72		Confirmed
Monitoring abnormal user/operator behavior	3.42	1.26	8.57		Confirmed
Risk-data transparency for agile teams	3.45	1.20	8.68		Confirmed
Multi-supplier IoT ecosystem risk management	3.37	1.27	8.31		Confirmed
Agile coordination among hardware, software, and network teams	3.35	1.14	7.88		Confirmed
Reducing battery or energy-source failure risks	3.21	1.25	7.61		Confirmed
Consumer privacy-risk assessment	3.38	1.20	8.17		Confirmed
Validation of sensor alert thresholds	3.37	1.13	8.15		Confirmed
Risk analysis of connected-node relationships	3.20	1.31	7.56		Confirmed
Flexible architecture for risk reduction	3.39	1.20	7.91		Confirmed
Sensor-data quality control	3.59	1.10	9.25		Confirmed
DevOps integration with IoT risk management	3.44	1.20	8.62		Confirmed

The second-round Delphi results showed that the most highly rated components were rapid identification of IoT-related risks, network-effect analysis of IoT node failure, integration of risks into the agile development cycle, and control of data-congestion risks. The findings indicated that the experts emphasized immediate risk detection, system-wide understanding of node failure effects, and agile integration of risk documentation and response mechanisms. Kendall's coefficient increased to 0.912 in the second round, with chi-square = 181.676, df = 81, and p = 0.000. This increase indicated a very strong level of consensus among the experts and confirmed the stability of the final model components.

Table 4. Kendall's Coefficient Results for the Two Delphi Rounds

Delphi Round	N	Kendall's W	Chi-Square	df	Asymp. Sig.	Interpretation
First round	31	0.703	166.410	81	0.000	Acceptable expert agreement
Second round	31	0.912	181.676	81	0.000	Very strong expert agreement

After completion of the Delphi rounds, the data were organized, transcribed, and supplemented with field notes. In the qualitative phase, the research data were analyzed through open, axial, and selective coding. The organizational realities

examined in this study were treated as dynamic, interpretive, and context-dependent phenomena. Therefore, coding was used to extract meaningful categories from the literature review, expert interviews, and comparative analysis. The initial 40 codes were reviewed and recoded, and the research team repeatedly compared the extracted categories to improve the quality and credibility of the findings. Expert judgment was also used as an important mechanism to confirm the theoretical and practical validity of the findings.

Through comparative integration, the 40 initial indicators were condensed into 17 integrated components. These integrated components represented broader dimensions of agile IoT-based risk management, including agile identification of IoT risks, rapid response to disruptions, real-time monitoring of equipment, data-driven risk prediction, cybersecurity and data protection, system resilience, hardware and energy risk control, communication and network risk management, agile configuration management, protocol and update risk management, node and behavior risk analysis, team agility, multi-supplier ecosystem management, quality-of-service evaluation, and DevOps integration.

Table 5. Integrated Codes and Categories in the Second Comparative Coding Stage

Integrated Component	New Code	Constituent Components
Agile identification of IoT risks	AC01	ARI01, ARI03, ARI14
Rapid response and reaction to disruptions	AC02	ARI02, ARI17, ARI25
Real-time and intelligent equipment monitoring	AC03	ARI05, ARI06, ARI22, ARI36
Data-driven risk prediction	AC04	ARI08, ARI09, ARI39
Cyber risk and data security management	AC05	ARI10, ARI11, ARI12, ARI35
System resilience and rapid recovery	AC06	ARI07, ARI38
Hardware and energy risk control	AC07	ARI13, ARI34
Communication and network risk management	AC08	ARI18, ARI19, ARI20, ARI21, ARI29
Physical-environment interaction risk management	AC09	ARI23, ARI24
Agile configuration management in IoT devices	AC10	ARI27, ARI28
Update and protocol risk management	AC11	ARI29, ARI18, ARI20
Risk analysis in node networks and behavior	AC12	ARI16, ARI30, ARI37
Transparency and free flow of risk information	AC13	ARI31
Team agility and cross-functional coordination	AC14	ARI26, ARI33
Multi-supplier ecosystem management	AC15	ARI32
Quality-of-service and data-performance assessment	AC16	ARI22, ARI36, ARI39
DevOps integration with IoT risk management	AC17	ARI40

In the next stage, the 17 integrated components were synthesized into six main components. These six components formed the final conceptual structure of the agile IoT-based risk management model. The first component, identification, monitoring, and prediction of IoT risks, covered risk detection, real-time monitoring, machine learning-based prediction, and network-node analysis. The second component, security, privacy, and cyber-threat management, included data protection, access control, cybersecurity, and risk-information transparency. The third component, rapid response, resilience, and recovery in agile environments, integrated crisis response and post-disruption recovery. The fourth component, network infrastructure, communication, and IoT quality-of-service management, focused on communication risks, data congestion, physical interactions, and infrastructure health. The fifth component, configuration, change, and DevOps integration management, addressed device configuration, firmware updates, communication protocols, and DevOps integration. The sixth component, organizational agility and multi-supplier ecosystem management, included team coordination, cross-functional agility, and supplier ecosystem management.

Table 6. Main Components of the Final Agile IoT-Based Risk Management Model

Main Component	Main Code	Constituent Components	Integration Logic
Identification, monitoring, and prediction of IoT risks	AM01	AC01, AC03, AC04, AC12	This component covers detection, real-time monitoring, machine learning, and connected-node analysis and forms the foundation of agile risk management.
Security, privacy, and cyber-threat management	AM02	AC05, AC13	This component includes security risks, access control, data protection, privacy, and transparency of risk information.
Rapid response, resilience, and recovery in agile environments	AM03	AC02, AC06	This component integrates rapid reaction, crisis management, recovery after failure, and resilience capacity.
Network infrastructure, communication, and IoT quality-of-service management	AM04	AC08, AC09, AC16	This component covers network risks, communication protocols, data congestion, physical-environment interaction, quality of service, and infrastructure health.
Configuration, change, and DevOps integration management	AM05	AC10, AC11, AC17	This component includes device configuration, firmware updates, protocol management, and integration of DevOps tools across the IoT lifecycle.
Organizational agility and multi-supplier ecosystem management	AM06	AC14, AC15	This component covers team coordination, cross-functional agility, and management of IoT suppliers in complex ecosystems.

Quality control of findings was carried out through repeated review, recoding, and classification of the extracted data. During content analysis, the research team reviewed the codes several times to ensure that the extracted concepts were conceptually meaningful and practically relevant. Expert review was used to strengthen theoretical and practical validity. The final coding structure showed that agile IoT-based risk management is not limited to technical monitoring or cybersecurity but includes a broader configuration of risk knowledge, resilience capacity, rapid response, organizational agility, quality of service, DevOps integration, and ecosystem coordination.

The system dynamics analysis was then conducted to examine the nonlinear and feedback-based relationships among the six final components. Traditional reductionist and econometric approaches are useful for linear and quantitative analysis, but they are limited in modeling complex systems with nonlinear feedback loops. This limitation is especially visible in IoT risk management, where cybersecurity, resilience, organizational agility, response speed, data quality, and network infrastructure interact dynamically. Therefore, a Causal Loop Diagram (CLD) was designed to identify the complex interactions among the key components of agile risk management. The CLD was then converted into a Stock and Flow Diagram (SFD) to enable simulation, sensitivity analysis, and scenario testing. Vensim PLE v7.3.5 was used as the main modeling and simulation software because it enables the definition of stocks, flows, auxiliary variables, rate variables, delays, and feedback structures.

The implementation process of the system dynamics model began with defining the research objective and model scope. The main objective was to present an agile IoT-based risk management model and simulate the long-term behavior of the system. The model scope included six key components: risk identification and prediction, rapid response and resilience, security and privacy management, organizational agility, network infrastructure and quality of service, and configuration-change and DevOps integration management. In the CLD design phase, the main system components were identified, reinforcing and balancing feedback loops were determined, causal relationships were drawn, and leverage points were detected. In the SFD conversion phase, the main stocks were defined as accumulated risk knowledge, system resilience capacity, security investment level, and organizational agility accumulation. The flows included the risk-data collection rate, risk-knowledge obsolescence rate, resilience improvement rate, resilience decay rate, security budget allocation rate, security consumption or depreciation rate, agility learning and improvement rate, and organizational rigidity rate. The auxiliary and rate variables included active quality of service, deployment velocity, and perceived risk intensity.

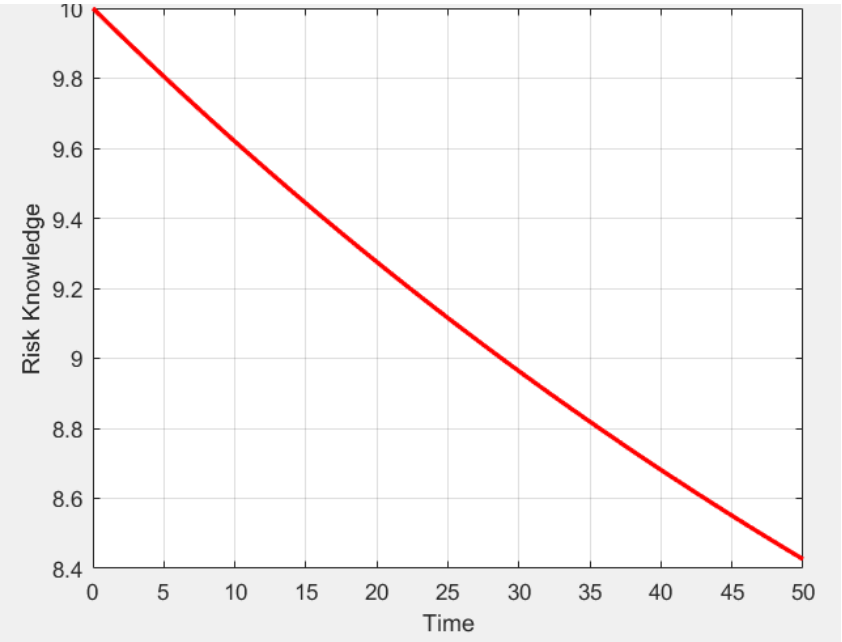

Figure 1. Accumulated Risk Knowledge Level

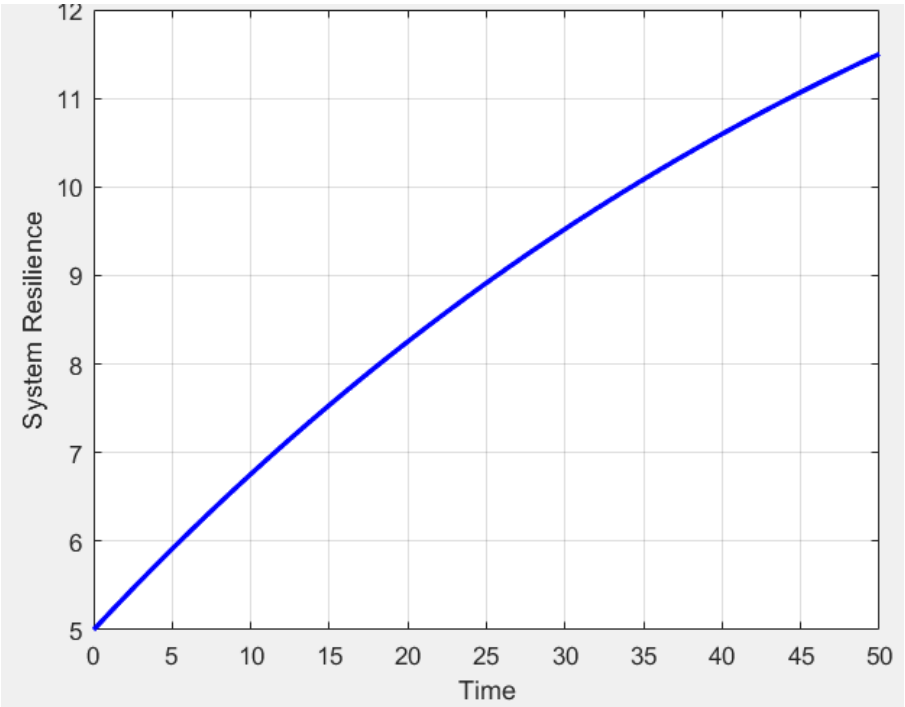

Figure 2. System Resilience Capacity

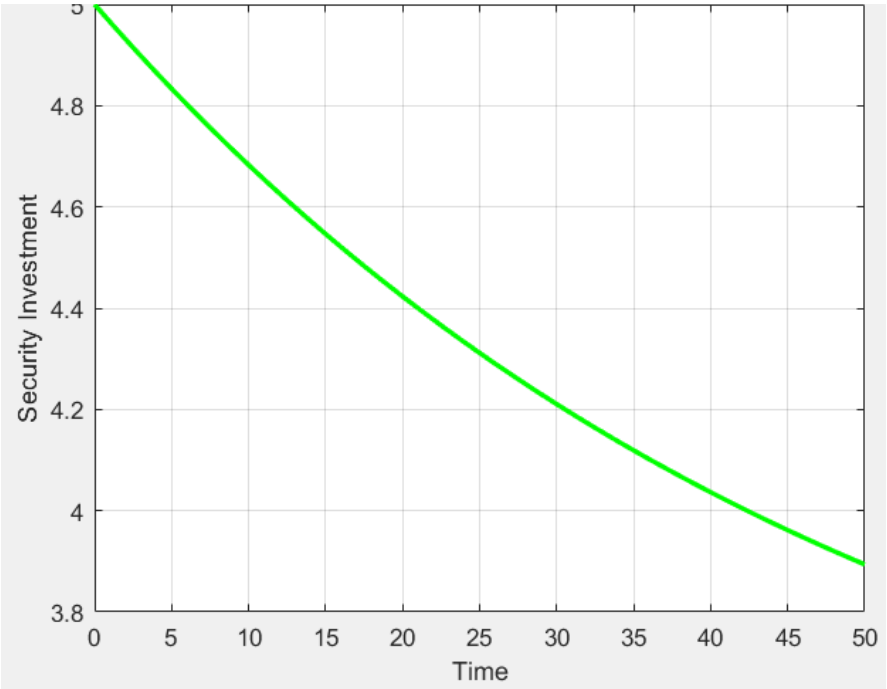

Figure 3. Security Investment Level

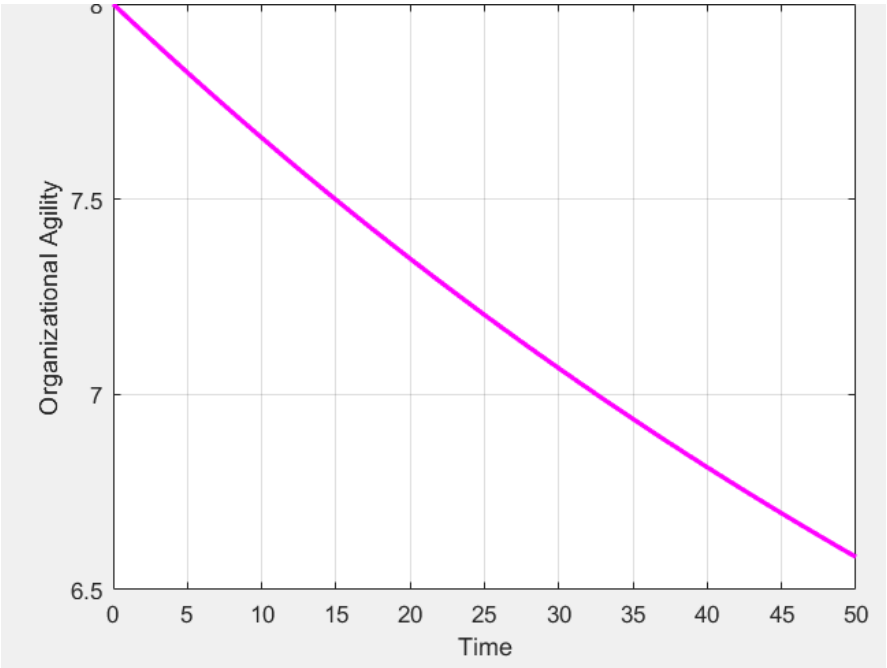

Figure 4. Organizational Agility Accumulation

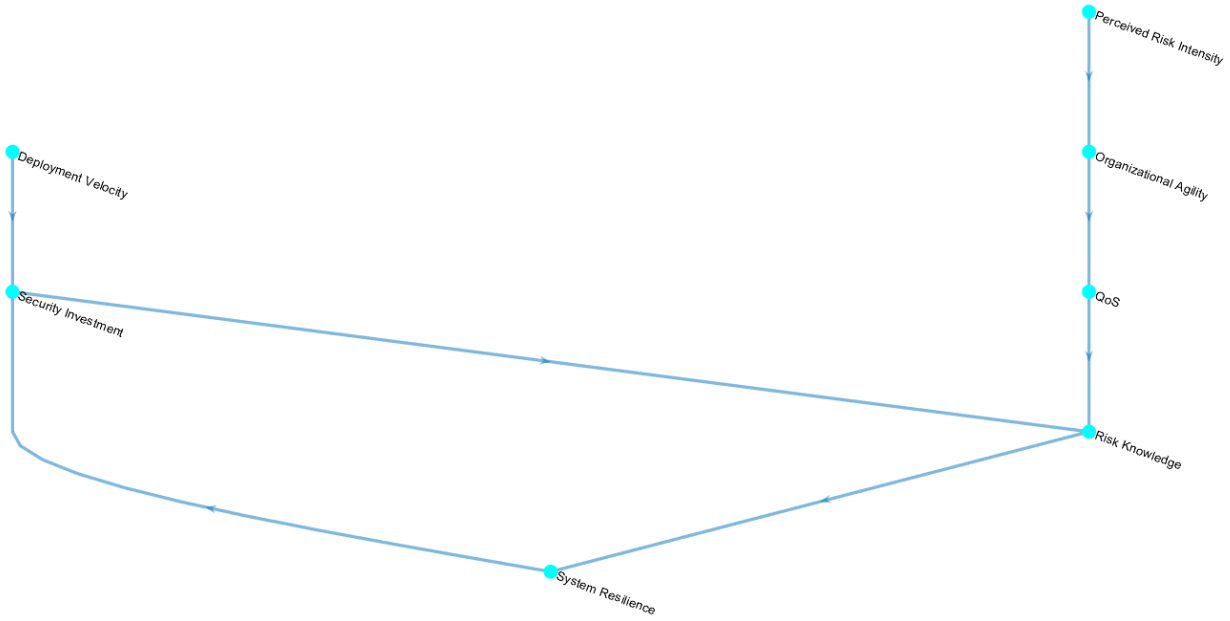

Figure 5. Causal Loop Diagram of Agile IoT Risk Management

The Causal Loop Diagram demonstrated the key interactions among the components of agile IoT-based risk management. Reinforcing feedback loops showed that higher organizational agility and accumulated risk knowledge mutually strengthen rapid response and resilience. In contrast, balancing loops indicated resource constraints and managerial trade-offs, such as the possibility that excessive security investment may reduce network quality of service and create a need for additional corrective actions. The interpretation of the CLD showed that increased accumulated risk knowledge improves rapid response capability and post-disruption recovery, which subsequently increases organizational agility. The conclusion derived from this diagram is that the system grows through reinforcing loops, while balancing loops preserve equilibrium. Therefore, the success of risk management depends on the organization's ability to balance these feedback structures.

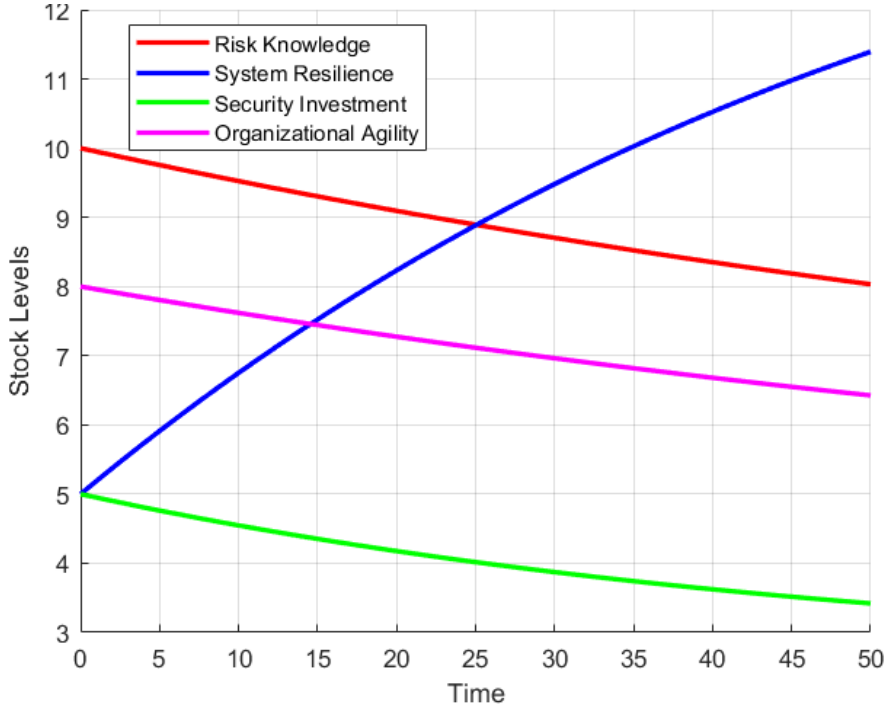

Figure 6. Dynamic Behavior of Each Stock Over Time

The dynamic stock behavior diagram displayed the time-based changes of accumulated risk knowledge, system resilience capacity, security investment level, and organizational agility. The simulation showed that accumulated risk knowledge

increased over time and approached a stable level. System resilience capacity also increased with delay and then stabilized. Security investment and organizational agility followed increasing trends, although both were sensitive to environmental parameters and internal feedback effects. These results indicated that the system tends to reach a dynamic equilibrium and that strengthening one stock can positively influence other stocks through feedback mechanisms.

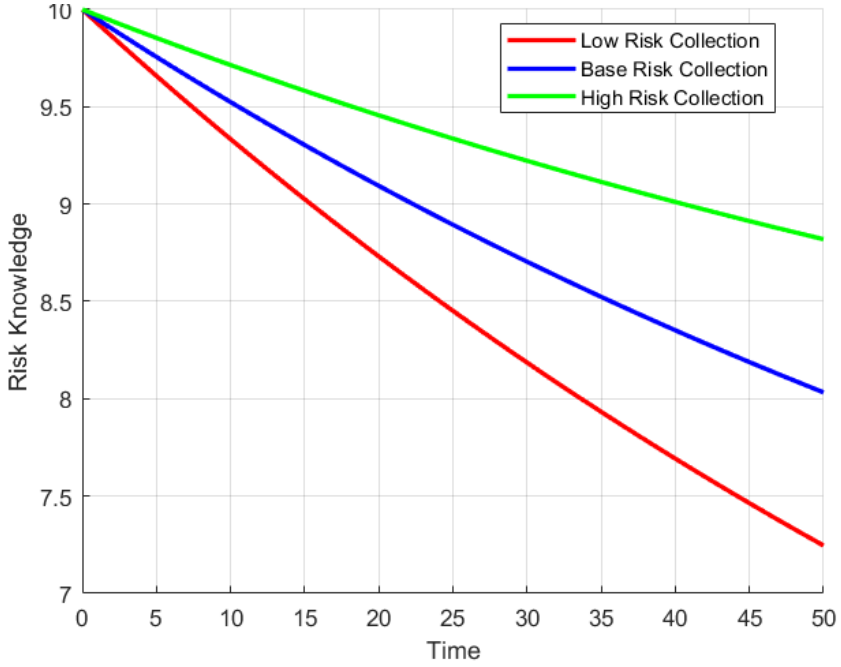

Figure 7. Scenario Analysis of the Agile IoT Risk Management Model

The scenario analysis compared system behavior under different managerial or parametric assumptions. By changing the risk-data collection rate and other key variables, the simulation showed how each scenario affected accumulated risk knowledge and organizational capabilities over time. The results indicated that increasing the risk-data collection rate accelerated the growth of accumulated risk knowledge and improved system resilience. Conversely, reducing this rate slowed stock growth and could weaken resilience and agility. Therefore, an appropriate scenario, especially one based on increased data collection and improved quality of service, can positively affect total system performance and guide managerial decisions.

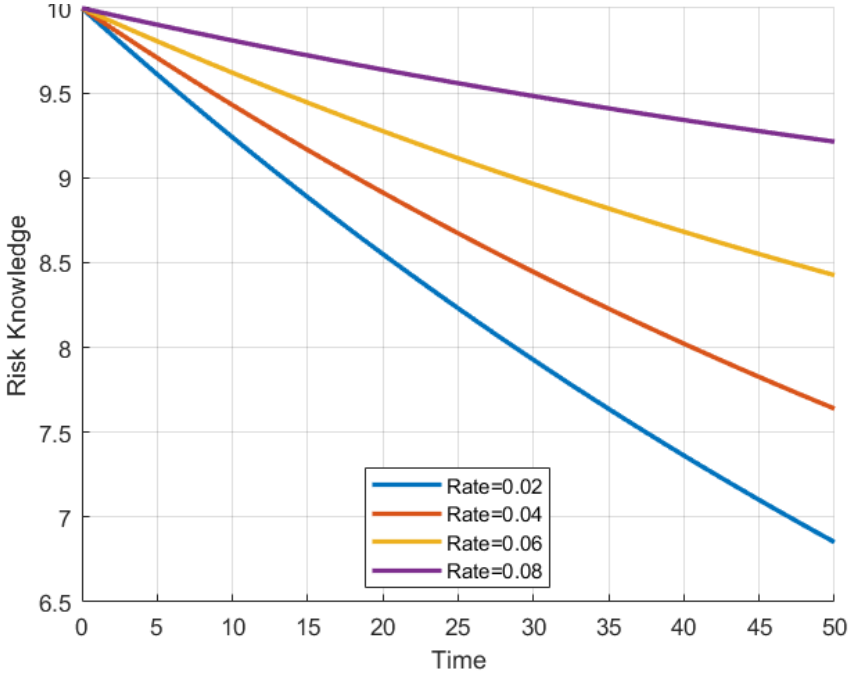

Figure 8. Sensitivity Analysis of the Agile IoT Risk Management Model

The sensitivity analysis showed the effect of changes in key parameters, such as the risk-data collection rate, on the behavior of system stocks. Small changes in critical parameters produced considerable differences in the long-term behavior of the stocks. More sensitive stocks, especially accumulated risk knowledge, reacted faster to parameter changes, while less sensitive stocks showed smoother fluctuations. These findings indicate that identifying sensitive parameters helps managers focus resources and attention on critical system variables and reduces the risk of unexpected performance decline.

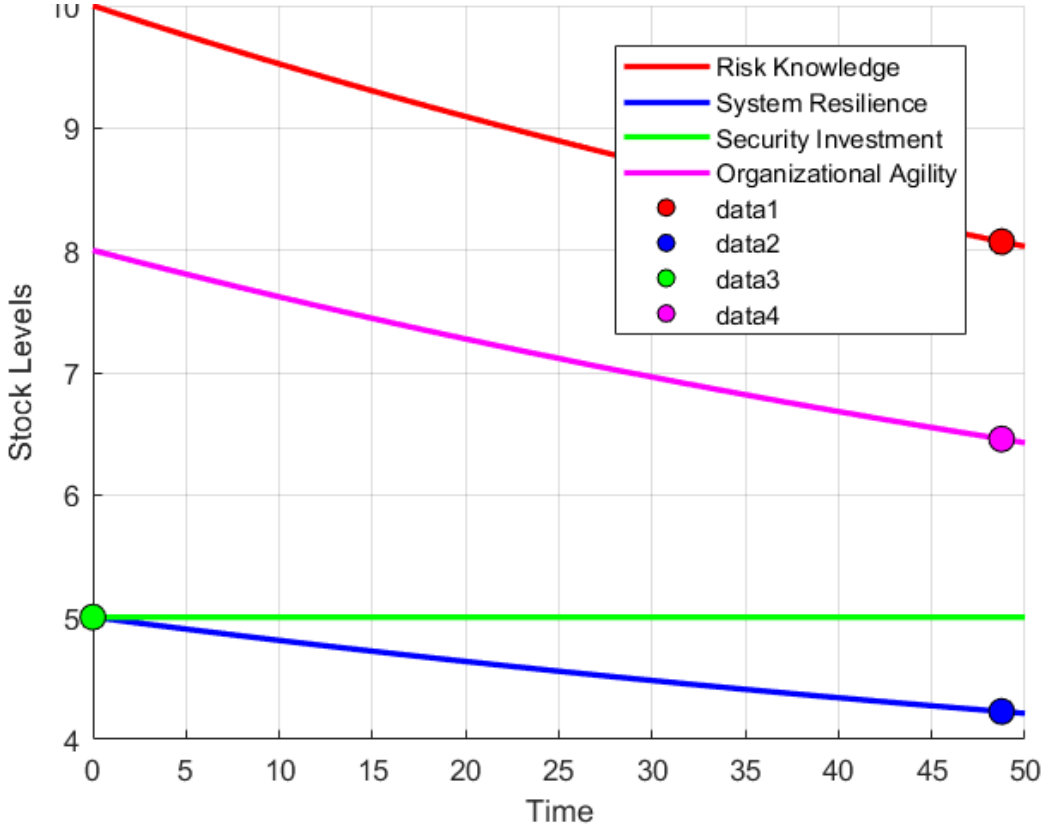

Figure 9. Leverage Points in the Agile IoT Risk Management Model

The leverage-points analysis identified the system variables that could produce the greatest positive change with the least intervention. The findings showed that accumulated risk knowledge and system resilience capacity had the greatest instantaneous changes at specific time points. These points represent managerial opportunities through which targeted interventions can improve system performance, resilience, and agility. Therefore, concentrating managerial resources on leverage points can improve system efficiency and support optimized resource-allocation strategies.

Figure 10. Final Causal Model of Agile IoT-Based Risk Management

The final causal model showed that agile risk management in IoT environments is not a linear process of "identification and response," but rather a dynamic system governed by reinforcing and balancing feedback loops. Reinforcing loops explain how organizational agility strengthens monitoring and prediction capability, which improves rapid response and recovery and further enhances agility. Balancing loops reveal managerial conflicts, especially the tension between security management and quality of service. Increased security focus may create network-quality challenges, which may increase operational risk and require further corrective actions. The final model therefore indicates that long-term resilience and stability in IoT ecosystems are achieved when risk management is treated as an inseparable part of organizational agility and as a self-correcting learning process that continuously adjusts itself based on feedback from monitoring, prediction, response, and recovery mechanisms.

4. Discussion and Conclusion

The findings of the present study demonstrated that agile risk management in Internet of Things (IoT) ecosystems is a multidimensional, dynamic, and adaptive process that requires simultaneous attention to technological, organizational, infrastructural, and security-related dimensions. The results of the Delphi analysis confirmed all identified indicators and showed a high level of expert agreement regarding the importance of rapid risk identification, continuous monitoring,

cybersecurity management, real-time response capability, organizational agility, and resilience enhancement. The increase in Kendall's coefficient from the first Delphi round to the second round indicated convergence of expert opinions and stability of the proposed model. These findings suggest that risk management in IoT environments cannot be effectively handled through isolated or static approaches; rather, it requires integrated and continuously evolving mechanisms capable of adapting to environmental uncertainty and technological complexity.

One of the most important findings of the study was the significance of real-time risk identification and intelligent monitoring systems in shaping agile risk management capability. The components related to rapid identification of IoT-related risks, continuous quality-of-service monitoring, anomaly detection, and machine learning-based prediction received high rankings from experts. This result confirms that modern IoT ecosystems depend heavily on continuous data collection and predictive analytics for maintaining operational continuity and resilience. These findings are consistent with studies emphasizing the role of intelligent and data-driven technologies in improving risk visibility and adaptive decision-making within digital infrastructures (Affia et al., 2023; Rahimi Kalvar & Ghasemi Hamadani, 2023). Previous research has shown that machine learning and intelligent monitoring mechanisms enable organizations to detect hidden vulnerabilities, reduce uncertainty, and improve rapid response capability in interconnected systems (Rezaeian & Mollahosseini, 2017). Similarly, studies on advanced persistent threat detection and cyberattack monitoring demonstrated that real-time anomaly detection systems significantly strengthen cybersecurity preparedness and operational resilience (Abu Talib et al., 2022; Al-Hamar et al., 2021). Therefore, the current findings reinforce the argument that predictive monitoring and intelligent analytics are essential pillars of agile IoT risk management.

Another major finding involved the central role of cybersecurity, privacy protection, and data security within IoT ecosystems. The results showed that cyber risk management, dynamic access control, sensor-data security, and privacy-risk assessment were among the most influential dimensions of the proposed model. This finding is understandable because IoT environments are highly vulnerable to cyber threats due to the extensive interconnectivity of devices, cloud platforms, and communication networks. The results align with previous studies indicating that cybersecurity has become one of the primary determinants of sustainability and resilience in digital ecosystems (Affia et al., 2023; Al-Dosari et al., 2023). Research on social engineering attacks and credential spearphishing also demonstrated that human-centered vulnerabilities remain critical challenges in connected systems (Al-Hamar et al., 2021; Aldawood & Skinner, 2020). The present findings extend these observations by showing that cybersecurity management must be integrated with organizational agility and operational responsiveness rather than treated as an isolated technical process. In other words, security systems should support rapid adaptation and continuous service delivery while simultaneously reducing vulnerabilities and protecting sensitive information.

The study also highlighted the importance of rapid response capability, resilience, and recovery mechanisms in agile IoT environments. The components related to service continuity, resilience capacity, reduction of response delay, and rapid recovery from disruptions were confirmed as key determinants of system stability and long-term performance. The system dynamics simulations further demonstrated that resilience accumulates gradually over time through continuous organizational learning and adaptive feedback mechanisms. These results are consistent with crisis-management studies emphasizing that resilient organizations are capable of absorbing shocks, adapting to disruptions, and recovering efficiently from operational failures (Abdel-Latif, 2023). The findings also correspond with research on dynamic simulation of IoT-based mitigation policies, which demonstrated that resilience-oriented strategies significantly improve long-term organizational stability and system sustainability (Al-Dosari & Fetais, 2023). From a theoretical perspective, the results support the idea that resilience should not be interpreted merely as resistance to disruption, but rather as an adaptive capability strengthened through learning, flexibility, and continuous feedback.

An important contribution of the present study lies in its identification of reinforcing and balancing feedback loops within the IoT risk-management system. The causal loop analysis showed that increases in accumulated risk knowledge improve rapid response capability and organizational agility, which subsequently enhance system resilience and further strengthen monitoring and prediction capabilities. This reinforcing mechanism indicates that agile organizations can create self-improving cycles of learning and adaptation. At the same time, balancing loops revealed the existence of trade-offs and managerial tensions, particularly between security investment and quality-of-service performance. Increased investment in security measures may improve system protection, but excessive restrictions or infrastructure burdens can negatively influence communication quality

and operational flexibility. These findings are highly consistent with system dynamics theory, which emphasizes that organizational systems evolve through interactions among reinforcing and balancing loops (Abdel-Latif, 2023; Ahmad & Sarjoughian, 2023). The findings therefore demonstrate the usefulness of system dynamics modeling for understanding nonlinear relationships and delayed effects within IoT ecosystems.

The integration of DevOps and agile configuration management was another critical aspect confirmed by the results. Experts emphasized that firmware updates, rapid configuration management, deployment velocity, and DevOps integration are necessary for sustaining agility and reducing operational risk in IoT environments. These findings align with previous studies on agile software development and hybrid Scrum-Extreme Programming methodologies, which argued that integrating risk management into development cycles significantly improves adaptability and project performance (Afshari & Gandomani, 2022; Azari & Javadani Gandomani, 2018). The present study extends this perspective into IoT ecosystems by demonstrating that configuration management and DevOps integration are not merely technical activities, but strategic mechanisms for maintaining organizational responsiveness and reducing system vulnerabilities. Rapid deployment and adaptive configuration processes allow organizations to respond more effectively to environmental changes, evolving cyber threats, and operational disruptions.

The findings also demonstrated the importance of organizational agility and coordination within multi-supplier ecosystems. Experts considered cross-functional coordination among hardware, software, and network teams as a critical factor in agile IoT risk management. This finding is highly relevant because IoT ecosystems involve multiple interconnected stakeholders, technologies, and infrastructures. Effective risk management therefore depends not only on technological capability but also on communication quality, organizational collaboration, and ecosystem-level coordination. These findings are supported by research on digital supply chains and IoT adoption, which identified collaboration capability and coordination mechanisms as major determinants of successful IoT implementation (Pourbagher et al., 2023). Similarly, studies on cloud-based knowledge management systems emphasized that digital transformation requires integrated organizational learning and collaborative adaptation (Khadivar & Dortaj, 2021). The current study contributes to this literature by demonstrating that organizational agility and ecosystem coordination directly influence resilience, response capability, and risk reduction in IoT environments.

Another significant result involved the identification of leverage points within the system. The sensitivity and scenario analyses revealed that accumulated risk knowledge and resilience capacity were among the most influential variables affecting long-term system behavior. Small changes in key parameters, such as risk-data collection rates, produced substantial effects on organizational agility and resilience. These findings support previous studies on quantitative risk analysis and simulation-based decision-making, which emphasized the importance of identifying sensitive parameters and strategic intervention points within complex systems (Acebes, Curto, et al., 2024; Acebes, Gonzalez-Varona, et al., 2024). The present study demonstrates that system dynamics modeling can effectively support managerial decision-making by revealing which variables produce the greatest positive effects with minimal intervention. This capability is particularly valuable in IoT ecosystems because organizations often face limited resources and must prioritize investments strategically.

The present findings also contribute theoretically to the evolution of risk management theory in digital environments. Contemporary theories increasingly emphasize adaptive, integrated, and ESG-oriented approaches to risk management (Abernikhina, 2025; Abernikhina et al., 2025). The current study supports this theoretical evolution by proposing a model in which cybersecurity, resilience, organizational agility, quality of service, DevOps integration, and ecosystem coordination operate as interconnected dimensions rather than isolated managerial functions. The findings suggest that successful risk management in IoT ecosystems requires a systemic and holistic perspective capable of integrating technological intelligence, organizational adaptation, and dynamic feedback mechanisms. This perspective differs fundamentally from traditional linear approaches that focus primarily on isolated risk identification and control procedures.

The findings additionally indicate that conventional reductionist and econometric methods are insufficient for analyzing the complexity of IoT-based systems. The nonlinear interactions among communication infrastructure, cyber threats, organizational learning, resilience accumulation, and quality-of-service dynamics require analytical approaches capable of capturing delayed effects and feedback-driven behavior. The successful application of system dynamics in the present study confirms the effectiveness of simulation-based methodologies for analyzing digital ecosystems and designing adaptive risk-management strategies. These results are aligned with previous simulation-modeling research emphasizing the usefulness of

dynamic analytical tools for understanding uncertainty, complexity, and organizational adaptation (Ahmad & Sarjoughian, 2023; Al-Dosari & Fetais, 2023).

Overall, the findings of this study demonstrate that agile IoT-based risk management should be understood as a continuously evolving and self-correcting system driven by organizational learning, intelligent monitoring, adaptive coordination, and dynamic feedback loops. Long-term organizational sustainability and resilience depend on the ability to balance security, agility, infrastructure quality, and operational responsiveness simultaneously. Organizations that rely solely on static risk-control procedures are unlikely to manage the complexity and uncertainty of interconnected digital ecosystems effectively. Instead, organizations require integrated and simulation-based approaches capable of supporting strategic adaptation, continuous learning, and proactive risk management in highly dynamic technological environments.

One limitation of the present study was that the data collection process relied heavily on expert judgments and qualitative evaluations, which may introduce subjective interpretations into the model-development process. Although the Delphi technique and repeated coding procedures were employed to improve validity and consensus, expert-based evaluations remain influenced by participants' experiences, professional backgrounds, and organizational contexts. Another limitation involved the geographical concentration of participants within selected industrial organizations, which may reduce the generalizability of findings to other industries or international contexts. Furthermore, the system dynamics simulation was based on conceptual and theoretical assumptions rather than real-time operational datasets, meaning that some dynamic relationships may behave differently in actual industrial environments. Time constraints and limited access to large-scale IoT operational infrastructures also restricted the possibility of conducting empirical longitudinal simulations in real organizational ecosystems.

Future research can extend the present model by integrating real-time operational data from industrial IoT systems and comparing simulation results across different industries such as healthcare, smart transportation, energy systems, and manufacturing. Researchers may also examine the role of emerging technologies such as blockchain, digital twins, edge computing, and generative artificial intelligence in improving agile risk management capability within IoT ecosystems. Another important direction involves developing quantitative structural equation models or hybrid machine-learning approaches to validate the causal relationships identified in the current study. Longitudinal studies examining the evolution of resilience and organizational agility over time would also contribute significantly to understanding adaptive risk-management mechanisms in digital environments. In addition, future studies could investigate cultural, organizational, and behavioral factors influencing the implementation of agile IoT risk-management systems.

From a practical perspective, organizations should establish integrated risk-management frameworks that combine real-time monitoring, predictive analytics, cybersecurity management, and agile response mechanisms within a unified operational structure. Managers should invest in organizational learning systems, cross-functional coordination mechanisms, and adaptive infrastructures capable of responding rapidly to disruptions and technological changes. Developing intelligent monitoring platforms and strengthening data-quality management can significantly improve resilience and decision-making capability. Organizations should also prioritize the integration of DevOps practices, configuration management systems, and dynamic feedback mechanisms in order to reduce operational vulnerabilities and improve deployment flexibility. Finally, managers should focus on identifying leverage points within their systems and allocate resources strategically toward variables that generate the greatest positive influence on resilience, agility, and long-term organizational sustainability.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abdel-Latif, A. (2023). System dynamics applications in crisis management. *Journal of Contingencies and Crisis Management*.

Abernikhina, I. (2025). The evolution of risk management theories in business: From classical to ESG-oriented digital models. *Economics of Systems Development*, *7*(2). https://doi.org/10.32782/2707-8019/2025-2-2

Abernikhina, I., Buriennikova, N., & Vakulenko, V. (2025). Digital-ESG integrated risk management: Historical development and theory. *Sustainability in Management Review*.

Abu Talib, M., Nasir, Q., Bou Nassif, A., Mokhamed, T., Ahmed, N., & Mahfood, B. (2022). APT beaconing detection. *Systematic Reviews*. https://doi.org/10.1016/j.cose.2022.102875

Acebes, F., Curto, D., de Anton, J., & Villafanez, F. (2024). Quantitative risk analysis using MCSimulRisk as a didactic tool. *ArXiv*. https://arxiv.org/abs/2405.20688

Acebes, F., Gonzalez-Varona, J. M., Lopez-Paredes, A., & Pajares, J. (2024). Beyond probability-impact matrices in project risk management: A quantitative methodology for risk prioritisation. *ArXiv*. https://doi.org/10.1057/s41599-024-03180-5

Affia, O. A., Nolte, A., & Matulevicius, R. (2023). IoT Security Risk Management: A Framework and Teaching Approach. *Informatics in Education*, *22*(4), 555-588. https://doi.org/10.15388/infedu.2023.30

Afshari, & Gandomani, T. J. (2022). A novel risk management model in the Scrum and extreme programming hybrid methodology. *International Journal of Electrical and Computer Engineering*, *12*(3), 2911-2921. https://doi.org/10.11591/ijece.v12i3.pp2911-2921

Ahmad, & Sarjoughian, H. S. (2023). An environment for developing simulatable AADL-DEVS models. *Simulation Modelling Practice and Theory*, *123*, 102690. https://doi.org/10.1016/j.simpat.2022.102690

Al-Dosari, H., Salayma, M., & Rahman, S. (2023). Dynamic simulation of IoT-based risk mitigation policies in industrial systems. *Simulation Modelling Practice and Theory*, *133*, 102695. https://doi.org/10.1016/j.simpat.2023.102695

Al-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629

Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise credential spearphishing attack detection. *Computers and Electrical Engineering*, *94*, 107363. https://doi.org/10.1016/j.compeleceng.2021.107363

Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, *177*(30), 1-11. https://doi.org/10.5120/ijca2020919744

Azari, K., & Javadani Gandomani, T. (2018). A Review of Risk Management in Agile Software Development Projects in XP and Scrum. Third Conference on the Latest Scientific Achievements in Computer Engineering, Soft Computing, and Modern Processing Technologies, Borujen. https://civilica.com/doc/787285

Feyzi, K., Asadi Qarabaghi, M., Olfat, L., & Taghavi Fard, M. T. (2020). Risk Management in Agile Software Development Projects: Designing a Process Model with a Qualitative Approach. *Quarterly Journal of the Iranian Management Sciences Association*, *15*(57), 1-27.

Kazemi, S., & Salajegheh, A. (2017). Using Agile Methodology for the Internet of Things (IoT). First International Conference on Electrical Engineering, Computer Science, and Information Technology, Hamedan. https://civilica.com/doc/678687

Khadivar, A., & Dortaj, F. (2021). Presenting a Framework for Successful Implementation of Cloud Computing-Based Knowledge Management Systems. *Management Research in Iran*, *20*(2), 93-118.

Mousaei, M., Javadani Gandomani, T., & Soltan Aghaei Koopaei, M. (2015). Investigating and Managing Risk in Agile Software Development and Presenting a New Solution to Improve Risk Management in Scrum-Based Projects. Second International Conference and Third National Conference on the Application of Modern Technologies in Engineering Sciences, Mashhad. https://civilica.com/doc/502199

Pourbagher, M., Valipour, P., & Ankari, M. (2023). Investigating Factors Affecting the Adoption of the Internet of Things (IoT) in the Digital Apparel Supply Chain Using FUZZY AHP and WASPAS Techniques. *Journal of Textile and Apparel Science and Technology*, *12*(4), 18-34. https://doi.org/10.22034/jtst.2024.177793

Rahimi Kalvar, H., & Ghasemi Hamadani, I. (2023). Analyzing the Role of Artificial Intelligence-Based Risk Management in Increasing Supply Chain Agility and Reengineering Capabilities.

Rezaeian, F., & Mollahosseini, M. (2017). Risk Management of Software Projects Developed with Agile Methodologies Based on Intelligent Agents. National Conference on Computer, Information Technology, and Artificial Intelligence Applications, Ahvaz. https://civilica.com/doc/762504