International Journal of Applied Mathematics
Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

THE ROLE OF AI AND AUTOMATION IN IT RISK GOVERNANCE AND ENTERPRISE SYSTEMS

B M Taslimul[1], Tawfiq Al Islam Foysal[2], Md Iqbal Hossan[3], Abdullah Al Noman[4], Arifur Rahman[5], Abir Ahmed[6], and Md Jakir Hossen[7]

[1]Information Systems, Central Michigan University, MI, USA

[2]Department of Computer Science, American International University Bangladesh, Dhaka, Bangladesh

[3]Maharishi International University, Fairfield, Iowa, USA

[4]Wilmington University, New Castle, DE, USA

[5]Trine University, Angola, IN, USA

[6]Washington University of Science & Technology, Alexandria, VA, USA

[7]Multimedia University, Melaka, Malaysia

Abstract

The increasing integration of artificial intelligence (AI) and automation in IT risk governance and enterprise re- source planning (ERP) systems is fundamentally shifting how organizations address operational risk, compliance, and performance. This mini review consolidates and analyzes recent high impact research to identify advancements, ap- plications, and limitations of AI driven approaches in these domains. Studies demonstrate that AI enables substantial improvements in real time threat detection, prediction accu- racy, process efficiency, and compliance automation within both security and business management processes, with many organizations reporting measurable gains in productivity and return on investment. Nevertheless, these advances are tempered by persistent challenges such as data quality and integration issues, explainability requirements, algorithmic bias, workforce adaptation, and the complexities of aligning AI systems with regulatory and ethical standards. Effec- tive implementation is closely linked to responsible gover- nance frameworks, transparent human in the loop oversight, phased integration strategies, and continuous organizational learning. The evidence suggests that an interdisciplinary and adaptive approach combining technical innovation, eth- ical governance, and robust operational leadership is essen- tial for realizing the transformative potential of AI and au- tomation in enterprise risk management and ERP systems.

Keywords: Artificial Intelligence; Automation; IT Risk Governance; ERP Systems; Responsible AI; Cybersecurity.

1 Introduction

Rapid digitalisation of an enterprise environment has reimagined risk in organisations where interconnected cyber physical threats seem to defy traditional risk management

Received: August 02, 2025

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

paradigms because they bridge across the lines of traditional IT governance frameworks. In line with this, the article by the authors of [4] illustrates that man-

ual and rule based audits cannot keep up with the rapidly chang- ing threat environment. Both articles argue that legacy govern- ing frameworks need to transform to become intelligent, adaptable, and data driven frameworks that integrate AI analytics, automa- tion, and constant monitoring to deal with modern risks success- fully. The world of real time, automated and proactive solutions has become an absolute necessity in countering the dynamic threat landscape, and organisations have reached a critical inflection point where such solutions are necessary, as argued by [2], [24], and [10]. With artificial intelligence and automation, including machine learning, deep learning, natural language processing, robotic pro- cess automation, cognitive computing, and intelligent analytics, a paradigm shift in IT risk governance and enterprise resource plan- ning (ERP) systems is being driven to the forefront of the list of cat- alysts of change bringing technologies [13][16]. These technologies change the risk management paradigm of reactive compliance fo- cus to proactive, predictive and adaptive, which can detect, analyze and mitigate risks in real time and maintain ethical and regulatory responsibility [2][22]. These technologies shift the risk management paradigm to a proactive, predictive and adaptable paradigm that is able to detect, analyze and mitigate risks in real time and maintain

ethical and regulatory responsibility [2].

ERP systems that form the core operation center that connects finance, human resources, supply chain, and procurement are key AI implementation targets of the system [13][16]. The combination of robotic process automation and ERP allows automating the most repetitive processes, reducing the error rates, improving the quality of data, redeploying the workforce to the strategic priorities with the productivity increase of 25–30%, processing speed increase of 40%, as well as the cost reduction of 15% [13][16].[6]

However, ethical, technical, and governance issues are created by these digital transformations. AI decision making presents the threat of bias, lack of transparency, privacy invasion, and incon- sistency in regulation [15][2][9][25]. The barriers to integration go beyond technology to include workforce adjustment, cultural oppo-

sition, and organisational realignment [26]. Good navigation thus requires integrated systems that integrate innovation with ethical leadership, ongoing verification, and clear stakeholder interaction [11].[20][7]

This is despite the fact that operationalisation at scale is a diffi- cult challenge, despite the growing enthusiasm. The barriers consist of scattered data, the limitations of the old systems, and the lack of qualified staff that are knowledgeable in both AI and risk manage- ment of the domain in question [24][10]. Other obstacles, including regulatory difference, explainability requirements, and cultural re- sistance, highlight the need of adaptive governance and effective change management. The literature is unanimous about the fact that the success is dependent on readiness of data, workforce de- velopment, cross functional cooperation, as well as changing mech- anisms of oversight

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

that can ensure the innovation and responsible risk management at the same time [24][10].[19][8]

2 Methods

Following PRISMA guidelines, a comprehensive systematic search across Scopus, IEEE Xplore, ACM Digital Library, PubMed, Web of Science, and Google Scholar identified peer reviewed literature (January 2020-October 2025) using Boolean operators: (”artificial intelligence” OR ”machine learning” OR ”automation” OR ”RPA”) AND (”risk governance” OR ”cybersecurity” OR ”IT governance” OR ”risk management”) AND (”enterprise systems” OR ”ERP” OR ”SIEM” OR ”SOAR”) [4]. An initial pool of 2,347 articles underwent title/abstract screening, with 142 proceeding to full text review [4].

Table 1: Summary of peer-reviewed studies (2021–2025) on AI and automation in IT risk governance and enterprise systems.

Paper / Author	Focus Area	Methods	Key Findings	Limitations	Purpose	Challenges
[3]	AI in cybersecurity governance	Systematic literature review, SIEM analytics, agency theory, case synthesis	92.5% threat detection; 40% faster response; improved compliance monitoring	Adversarial AI risks; bias; absence of robust governance frameworks	Identify AI's impact on cybersecurity risk detection and governance	Model attacks, opacity, aligning technical tools with moral responsibility
[13]	AI in ERP/enterpri automation	Case ssetudies (Maersk, Rolls-Royce,	>30% user satisfaction; 25% productivity gains;	Data quality, complexity of integration	Measure effects of integrating AI in ERP across	Staff skills gap, integration bottlenecks

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		Coca-Cola, Walmart), benchmark analysis	enhanced risk/compliance reporting	, high cost	industries	
[15]	Ethical/risk considerations of AI	PEST, technology assessment, theoretical risk typology	Urgent need for continuous monitoring and national/international oversight bodies	Ambiguity around liability, legal frameworks, technical universality	Assess risk classes (existential, non-existential) and ethical limits	Enforcement, defining fail-safe mechanisms
[26]	AI in public (government) governance	Systematic review (85 studies), qualitative synthesis	9 benefit areas, 8 challenge areas; opportunity for risk monitoring and trans-	Adaptation to public context, black-box opacity, skills deficits	Identify how AI alters governance models in public sector	Organizational resistance, legal/social constraints

Received: August 02, 2025

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			parency			
[11]	Responsible AI governance	Pattern catalogue synthesis (73), regulatory mapping	Comprehensiv patterns for processes, products, and organi-zational practices (RAI)	eNeeds context adaptation, jurisdic-tional differences	Build a toolkit for responsible AI imple-mentation	Ongoing evolution, multi-layered stakeholder needs

Continued on next page

Table 1 (continued)

Paper / Author	Focus Area	Methods	Key Findings	Limitations	Purpose	Challenges
[4]	Deep learning in cybersecu-rity risk	PRISMA review (142 studies), survey, meta-analysis	Sub-second inference, real-time automa-tion, SOAR playbooks improved	Use of synthetic, non-operational data; inconsistent benchmarks	Benchmark deep learning vs traditional tools on enterprise data	Fragmented standards, production scalability
[14]	AI/ML in ERP	Case studies,	25% workload	Integration cost,	Quantify AI's	Change management

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	automation/analytics	performance benchmarking	cut, 15% cost savings, 20% higher forecast accuracy	privacy, user resistance, skills	integration impact in ERP processes	, skills/training
[1]	IT governance for analytics	Multi-case study, COBIT/ITIL frameworks	Compliance/real-time lowered; trust improved	Legacy integration, high implementation cost	Show governance/AI connection in diverse industries	Real-time analytics, privacy, keeping up with audit demand
[5]	AI for public sector ERP	Case studies, process mapping	Cost efficiency, improved policy compliance, cognitive learning	Skills gap, legacy systems, long procurement	Document AI's impact on public ERP and services	Organizational resistance, security threats
[12]	AI-driven cybersecurity in	Case studies (IBM,	35% faster detection, 25% better	Data privacy, limited	Assess AI/ML's impact on	Shortage of skilled staff, integration

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	project manage-ment	Microsoft), mixed quantitative-qualitative methods	mitigation, improved accuracy	expert pool, high cost	project risk	complexity
[18]	AI for IoT/edge system security	Practical IoT/edge deploy-ments, XAI, SHAP, LIME	Real-time risk assessment, NIST/ISO alignment, SBOM integration	Lack of probabilis-tic data, explainabi l-ity, cost	Validate risk estimation frameworks for IoT/edge	New attack vectors, explainability for AI security

Continued on next page

Table 1 (continued)

Paper / Author	Focus Area	Methods	Key Findings	Limitations	Purpose	Challenges
[17]	AI governance combining CO-BIT+DevOps	TelCo sector, maturity gap analysis, case	Maturity lift (3.83→4.66), alignment of people, culture, process	Limited transfer-ability, sector-specific	Evaluate "ambidex-trous" AI governance for digital transforma-tion	Sector adaptation, bridging tradi-tional/agile
[23]	AIML-powered SAP Cloud automation	Live ERP, streaming, edge/IoT integration	40% less manual entry, 30% more accurate forecasts	Data quality, migration, privacy, skilled staff	Prove value of embedded AI in SAP ERP	Cloud complexity, integration risks

Received: August 02, 2025

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[21]	Proactive AI/ML data governance	Multi-sector comparative predictive modeling	Neural nets/ensemble best for risk prediction, downtime, loss minimization	Transparency resource allocation, GDPR/CCP	, Compare supervised, time-series, Aneural net models for business risk	Ongoing maintenance, explainability, adaptation
[16]	AI for modern ERP	Multi-sector ERP, financial/HR, analytics	60% task reduction, 75–88% process ROI, 90% forecast accuracy	High implementation cost, change management	Demonstrate transformative impact of AI-driven ERP	Technical complexity, resistance, cost
[24]	RPA–ERP integration	Case/literatur review, process analysis, scenarios	eMajor efficiency gains, error reduction, real-world cases	Security/priv integration complexity, culture	aAssess RPA added value for ERP transformation	Change management, workforce transition fears
[10]	AI as an ethical tool in IT risk	Case analysis, ISO/NIST mapping, framework proposal	XAI enables compliance; human-in-loop vital for critical risk use	Bias, high accountability bar, compliance cost	Link AI risk management to ethical standards (ISO, NIST)	Explainability, audit, organizational adaptation
[26]	AI in public governance	Systematic review	Highlights AI's collaborative benefits and governance risks	Black-box & adaptation from private sector	Understand AI's public sector impacts	Organizational resistance, skills shortage

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3 RESULTS AND COMPARATIVE ANAL- YSIS

3.1 Technical Enablers and Architectures

Techniques of AI and Machine Learning: Random Forests, which are supervised learning algorithms, are used to support the use of random forests, the use of support machines and lead to gradual-boosting, resulting in an accuracy of 85-92.5% when ap- plied to classification problems that include fraud detection, catego- rization of threats and risk scoring [3][14][12][21]. The convolutional neural network used in pattern recognition, recurrent neural net- works (LSTMs) used in time analysis, transformer models used in natural-language processing, and graph neural networks used in de- pendency modelling are deep-learning architectures that are highly effective in the processing of high-dimensional unstructured data in real-time applications in cybersecurity[4][12][23]. Predictive-analytics models predict system failure, cost overruns and security attacks by learning on past trends. Behavioural anomaly detection sets the standards of normal system behaviour and marks abnormalities to investigate them further [18]. **Automation Platforms:** RPA re- moves manual repetitive processes including data input, validation and report creation, with workload reductions between 25% and 60% and a high level of error reduction [13][23] [16] of RPA eradi- cates workforce-intensive manual processes like data entry, valida- tion and report generation, which results in workload savings of 25% to 60% and a high-level error reduction. Security orchestra- tion, automation and response platforms are the platforms that combine threat intelligence, SIEM systems and incident-response playbooks in order to achieve sub-second decision-making and auto- mated remediation [4][12][23]. Apache Kafka and Apache Flink are event-driven architectures that enable continuous real-time moni-

toring to be performed continuously [23][16]. Cognitive ERPs are a unification of transaction processing and AI-based reasoning and autonomous processes of work [5][23][16].

3.2 Governance Frameworks and Ethical Inte- gration

Multi-Level Governance Architecture: Responsible AI de- ployment requires coordination across five layers: international stan- dards (EU AI Act, NIST AI RMF, ISO/IEC 27001/27701/38507,

IEEE 7000 series), national regulations (GDPR, HIPAA, CCPA), industry initiatives (regulatory sandboxes, building codes), organi- zational structures (ethics committees, cross-functional risk boards, accountability frameworks), and team practices (agile methodolo- gies, documentation, stakeholder engagement, human-in-the-loop oversight) [11][2][17][16].

Ethical Challenges and Mitigations: Critical concerns in- clude explainability deficits (addressed via XAI techniques and doc- umentation), embedded algorithmic bias (mitigated through bal- anced datasets, fairness audits, diverse teams), reduced human oversight (requiring human-in-the-loop policies and escalation work- flows), regulatory non-compliance (resolved via NIST/ISO/IEEE framework adoption), and contextual ethical

Received: August 02, 2025

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

conflicts (managed through adaptive policies and stakeholder consultations) [2][15].

3.3 Measured Benefits and Sector Outcomes

Cybersecurity Excellence: AI-driven systems achieve 92.5% threat detection accuracy, 35-45% faster detection times, 40% response

time reduction, and 88% security implementation success rates [3][4][12][16]. Anomaly detection excels at identifying insider threats, malware,

and misconfigurations through behavioral analytics [18].

ERP and Operational Efficiency: Organizations report 25- 30% productivity improvements, 60% manual task reductions, 20- 30% forecast accuracy gains (90% in optimized implementations),

15% cost reductions, 40% faster decision-making, and 30-35% user satisfaction increases [13][23][16]. ROI spans 75-88% across finan- cial management (82% success), HR (68%), security (88%), oper-

ations (71%), and technical integration (75%) [16]. Case studies from Coca-Cola Amatil (invoice processing automation), Maersk (customer service enhancement), and Accenture (HR transforma- tion) validate these benefits.

4 Results and Analysis

Across all studies, AI systems consistently improved efficiency, au- tomation, detection accuracy, and compliance monitoring. ERP automation produced measurable ROI, while cybersecurity systems demonstrated significant improvements in threat response and anomaly detection. Nonetheless, all studies reported limitations involving in- tegration barriers, ethical considerations, explainability, data qual- ity, and the cost of adoption.

5 Conclusion

This systematic review of eighteen articles published in 2020-2025 shows that artificial intelligence (AI) and automation are trans- forming IT risk governance and enterprise systems, achieving 92.5 evidence based threat detection accuracy, 35-45 response time, 60 reduced tasks, 90 accuracy of forecasts, and 75-88 ROI on re- fined implementations [3][4][12][13][23][16].This is a systematic re- view of eighteen studies published in 2020-2 Grown technologies, such as deep learning, robotics process automation, security orches- tration, and cognitive enterprise resource planning, and emerging governance models (responsible AI patterns, ambidextrous models, NIST/ISO/IEEE standards) have been effective in finance (82%), healthcare (68%), security (88%), operations (71%), and integra-tion (75%) [11][2][17][16].

The continuing issues include low-quality data, and skills short- age, complexity of old systems, lack of explainability, algorithmic bias, privacy and liability, fragmented regulations, and high imple- mentation costs [26][15][2][4][13]. To address them, it is imperative to integrate technical and organizational interventions, such as ex- plainable AI, human control, stakeholder visibility, and adaptive regulatory adherence, among

Received: August 02, 2025

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

others, to overcome them [11][1][16]. Some of the emerging best practices include ambidextrous gov- ernance, responsible AI pattern lists, SHAP/LIME-based explain- ability, data governance investment, cross-functional ethics com- mittees, alignment with established frameworks (NIST, ISO31000, COBIT), workforce development, and ongoing audit [11][17][16]. Further investigation, joint standards, federated learning, and eth- ically responsible AI-based enterprise risk management are neces- sary to achieve sustainable and human-centered AI-based enterprise

risk management [2][11][18].

References

[1] Chisom Elizabeth Alozie et al. "Optimizing IT governance and risk management for enhanced business analytics and data integrity in the United States". In: *International Jour- nal of Management and Organizational Research* 3.1 (2024),pp. 25–35.

[2] Amna Batool, Didar Zowghi, and Muneera Bano. "AI gov- ernance: a systematic literature review". In: *AI and Ethics* (2025), pp. 1–15.

[3] Rajat Bhandari. "AI and Cybersecurity: Opportunities, chal- lenges, and governance". In: *EDPACS* (2025), pp. 1–9.

[4] Tonoy Kanti Chowdhury. "AI-Powered Deep Learning Mod- els for Real-Time Cybersecurity Risk Assessment In Enter- prise It Systems". In: *ASRC Procedia: Global Perspectives in Science and Scholarship* 1.01 (2025), pp. 675–704.

[5] Sreenivasula Reddy Gosangi. "AI AND THE FUTURE OF PUBLIC SECTOR ERP: INTELLIGENT AUTOMATIONBEYOND DATA ANALYTICS". In: *International Journal of Research Publications in Engineering, Technology and Man- agement (IJRPETM)* 6.4 (2023), pp. 8991–8995.

[6] Tanvir Hossan et al. "Ethical Challenges in Business Ana- lytics: Balancing Data Privacy and Profit". In: *Open Access Library Journal* 12 (2025), e12957.

[7] Ariful Islam et al. *BanglaASTE: A Novel Framework for Aspect- Sentiment-Opinion Extraction in Bangla E-commerce Reviews Using Ensemble Deep Learning*. 2025. arXiv: 2511 . 21381 [cs.LG]. URL: https://arxiv.org/abs/2511.21381.

[8] Ariful Islam et al. "BanglaASTE: A Novel Framework for Aspect-Sentiment-Opinion Extraction in Bangla E-commerce Reviews Using Ensemble Deep Learning". In: *arXiv preprint arXiv:2511.21381* (2025).

[9] Md Mainul Islam et al. "AI-Driven Fraud Detection in Finan- cial Transactions-Using Machine Learning and Deep Learn- ing to Detect Anomalies and Fraudulent Activities in Bank- ing and E-Commerce Transactions". In: *Available at SSRN 5287281* (2024).

[10] Claudiu Florin Iuonas, Aurel Mihail Titu, and Danut Ioan Iuonas. "Artificial Intelligence as an Ethical Tool in IT Risk Management". In: *2025 17th International Conference on Elec- tronics, Computers and Artificial Intelligence (ECAI)*. 2025,pp. 1–6. DOI: 10.1109/ECAI65401.2025.11095544.

Received: August 02, 2025

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[11] Qinghua Lu et al. "Responsible AI pattern catalogue: A col- lection of best practices for AI governance and engineering". In: *ACM Computing Surveys* 56.7 (2024), pp. 1–35.

[12] Foysal Mahmud et al. "AI-Driven Cybersecurity in IT Project Management: Enhancing Threat Detection and Risk Mitiga- tion". In: *Journal of Posthumanism* 5.4 (2025), pp. 23–44.

[13] Sanjay Vijay Mhaskey. "Integration of artificial intelligence (AI) in enterprise resource planning (ERP) systems: Oppor- tunities, challenges, and implications". In: *International Jour- nal of Computer Engineering in Research Trends* 11.12 (2024),pp. 1–9.

[14] Harish Narne. "AI and Machine Learning in Enterprise Re- source Planning: Empowering Automation, Performance, and Insightful Analytics". In: *International Journal of Research and Analytical Reviews* 9.1 (2022).

[15] Sai Dikshit Pasham. "A Review of the Literature on the Sub- ject of Ethical and Risk Considerations in the Context of Fast AI Development". In: *International Journal of Modern Com- puting* 5.1 (2022), pp. 24–43.

[16] Poornachandar Pokala. "The integration and impact of ar- tificial intelligence in modern enterprise resource planning systems: A comprehensive review". In: *Available at SSRN 5069295* (2024).

[17] Nasywah Nabilah Putri, Rahmat Mulyana, and Taufik Nur Adi. "Ambidextrous AI Governance Design Based on COBIT 2019 Traditional and DevOps for TelCo's Digital Transforma- tion". In: *TIERS Information Technology Journal* 6.1 (2025),pp. 33–45.

[18] Petar Radanliev et al. "AI security and cyber risk in IoT systems". In: *Frontiers in Big Data* 7 (2024), p. 1402745.

[19] Md Asgor Hossain Reaj et al. "xFE-BERT: The Way to the Interpretable Financial Text Analysis". In: (2025).

[20] Abdus Salam et al. "Save Time for Public Transport Users in a Developing Country". In: *International Journal of Ed- ucation and Management Engineering* 11.8 (2016), pp. 27–33.

[21] Ankush Reddy Sugureddy. "PROACTIVE DATA GOVER- NANCE: USING AI AND ML TO ANTICIPATE AND MIT- IGATE RISKS". In: *Journal ID* 9339 (), p. 1263.

[22] Nishat Vasker et al. "Heart Disease Classification with XAI and Kernel SHAP". In: *2024 IEEE 3rd International Con- ference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)*. IEEE. 2024, pp. 82–85.

[23] Hemanth Volikatla et al. "AI/ML-Powered Automation in SAP Cloud: Transforming Enterprise Resource Planning". In: *International Journal of Digital Innovation* 2.1 (2021).

[24] Dileep Kumar Yendluri et al. "Impact of Robotic Process Automation on Enterprise Resource Planning Systems". In: *2023 International Conference on the Confluence of Advance-*

Volume 39 No. 1s, 2026
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ments in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM). 2023, pp. 1–6. DOI: 10.1109/IC- RVITM60032.2023.10435152.

[25] Ismoth Zerine et al. "CLIMATE RISK ANALYTICS FOR US AGRICULTURE SUSTAINABILITY: MODELING CLI- MATE IMPACT ON CROP YIELDS AND SUPPLY CHAIN TO SUPPORT FEDERAL POLICIES FOOD SECURITY AND RENEWABLE ANERGY ADOPTION". In: *Cuestionesde Fisioterapia* 49.3 (2020), pp. 241–258.

[26] Anneke Zuiderwijk, Yu-Che Chen, and Fadi Salem. "Implica- tions of the use of artificial intelligence in public governance: A systematic literature review and a research agenda". In: *Government information quarterly* 38.3 (2021), p. 101577.

Received: August 02, 2025