Annals of "Dunarea de Jos" University of Galati
Fascicle I. Economics and Applied Informatics
Years XXXI – nº3/2025
ISSN-L 1584-0409 ISSN-Online 2344-441X
www.eia.feaa.ugal.ro

DOI https://doi.org/10.35219/eai15840409569

Intelligent Automation and Machine Learning as Key Drivers of Digital Transformation in SMEs under Emerging Economic Risks

George Chirita★, Marian Barbu★★

ARTICLE INFO

Article history:
Received December 10, 2025
Accepted December 28, 2025
Available online December 2025

JEL Classification
O33, M15, L26, D81

Keywords:
intelligent automation, machine learning, digital transformation, SMEs, economic risk, artificial intelligence adoption

ABSTRACT

This article investigates how intelligent automation (AI) and machine learning (ML) act as key enablers of digital transformation in small and medium-sized enterprises (SMEs) in the face of emerging economic risks. Based on a critical review of recent literature and a bibliometric mapping conducted on data from the Web of Science Core Collection, the study shows that the research agenda is strongly focused on the AI/ML–SME triad and on risk-related predictive applications, e.g., financial fragility, insolvency, credit risk, but the mechanism by which ML capabilities are transformed into end-to-end operational outcomes and economic resilience remains poorly explained. The article proposes a "risk-aware" conceptual framework that treats AI and ML as an integrated system: ML generates cognitive signals, such as predictions, recommendations, anomaly detection, including GenAI/NLP, and AI operationalizes these signals into orchestrated, monitored, and auditable processes. Implementation typologies are identified (from point automation in back-office and augmented analytics, to end-to-end hyperautomation and GenAI-based front-office automation) and the mechanisms through which AI–ML can reduce vulnerabilities (efficiency, response time, resource optimization, continuity) or introduce new risks (drift, bias, security, compliance, vendor dependency) are discussed. The results highlight the decisive role of organizational mediators, such as data quality, skills and AI literacy, governance, auditability and vendor management, in differentiating between value creation and risk amplification. The contribution of the study lies in the explicit integration of the "risk-aware" economic perspective in the assessment of AI–ML adoption in SMEs and in the formulation of application directions for responsible and scalable implementations.

1. Introduction

The digital transformation of small and medium-sized enterprises (SMEs) has entered a phase of accelerated intensification, fueled by the convergence of intelligent automation (hyperautomation) and machine learning (ML). From an operational perspective, this convergence marks the transition from predominantly deterministic, rule-based automation (such as Robotic Process Automation – RPA) to adaptive automation, capable of operating with semi-structured or unstructured data, learning from organizational contexts and supporting managerial decision-making through prediction, recommendation and anomaly detection (including through NLP and generative models). The integration of AI/ML into end-to-end processes is no longer described in specialist articles as an incremental optimization, but more as a mechanism for reorganizing workflows, responsibilities and coordination capabilities, with possible potential effects on the productivity and competitiveness of firms (Ng et al., 2021; OECD, 2025a).

In parallel, a series of economic articles, but also public policy reports outline AI as a technology with generalized effects, a general-purpose technology. The authors argue that it is capable of simultaneously influencing productivity, innovation dynamics and the distribution of competitive advantages between firms. However, it can be observed that the diffusion of AI remains uneven, while the gaps between SMEs and large companies tend to persist, sometimes even widen, depending on digital maturity, access to data, skills and even financing. A series of specialized reports summarize these differences both at a first level of adoption, but also at a level related to the ability to transform the use of AI into measurable economic performance, highlighting structural barriers specific to SMEs (Filippucci et al., 2024; Kergroach, 2025; OECD, 2025a).

For SMEs, this transition takes place in a context of emerging economic risks that increase pressure on efficiency and resilience: demand volatility, cost pressures, supply chain fragility, geopolitical and geoeconomic

★, ★★Dunarea de Jos University of Galati Romania. E-mail addresses: gechirita@ugal.ro (G. Chirita – Corresponding author), marian.barbu@ugal.ro (M. Barbu).

uncertainty, as well as financing constraints. At the macro level, recent assessments of global risks describe an increase in fragmentation and geoeconomic tensions, with indirect effects on market stability and operational continuity, dimensions to which SMEs are usually more exposed due to their reduced shock absorption capacity (WEF, 2025a).

In addition, regulatory uncertainty is becoming a central variable in AI-based digital transformation strategies. In the European space, the adoption of the AI Act (Regulation (EU) 2024/1689) introduces a comprehensive framework, with differentiated obligations depending on the level of risk of AI systems and with phased implementation, which can generate both institutional clarity and compliance costs and new governance needs (e.g. documentation, data management, traceability and responsibilities). For SMEs, the net effect depends on their positioning (users vs. developers, integration into high-risk systems vs. general use) and the ability to internalize proportionate compliance processes (European Commission, 2025).

In this equation, the relationship between intelligent automation and ML is best understood as a relationship of functional complementarity. Intelligent automation is described in recent research as an architecture that combines: (i) automation of repetitive tasks (RPA and workflow automation), (ii) cognitive capabilities (ML, NLP, computer vision, generative models), and (iii) end-to-end process orchestration, including monitoring, governance, and continuous improvement. In this logic, ML does not replace automation, but "lifts" it from rigid execution to adaptive orchestration: it classifies and extracts information from documents, anticipates demand, optimizes inventory, detects anomalies/fraud, recommends actions, and supports real-time prioritization. Recent conceptual modeling of AI–RPA integration emphasizes that value does not come exclusively from "quick wins," but from coupling efficiency with data-driven decisions and reconfiguring responsibilities between people and systems (Kitsantas et al., 2024; Patrício et al., 2025).

For SMEs, this complementarity has double economic significance. On the one hand, ML extends automation beyond strictly standardized activities, reducing coordination costs and execution time in processes where data is heterogeneous (emails, texts, images, conversations). On the other hand, intelligent automation operationalizes ML in auditable flows, transforming predictions and recommendations into observable results (operational KPIs, error reduction, better response times, service improvement). At the same time, the literature warns that, in the absence of quality data, adequate infrastructure and AI literacy, integrating ML into automation can amplify errors, increase the risk of non-compliance and introduce technological dependencies on suppliers (OECD, 2023).

The "structural vulnerability" of SMEs to rapid technological transitions derives from limited resources and the reduced capacity to simultaneously manage investments, organizational change and risks. European reports on the digitalization of SMEs identify recurring barriers: lack of financing, digital skills' deficit, insufficient infrastructure and cybersecurity concerns (Eurofound and Cedefop, 2025).
At the same time, a series of analyses dedicated to the adoption of AI in SMEs explicitly highlight the role of connectivity, "AI-enabling" inputs (data, infrastructure, access to solutions), skills and financing as preconditions for diffusion, even proposing taxonomies of adopters according to digital maturity and complexity of use (OECD, 2025).

The skills dimension is essential because AI/ML-based digital transformation goes beyond the scope of technological adoption and involves a reconfiguration of work, including the redistribution of roles, the redefinition of tasks, the recalibration of responsibilities and the adaptation of organizational control mechanisms. Recent analyses of the labor market and skills demand indicate that occupations with high exposure to AI tend to increasingly require digital, cognitive and socio-managerial skills, and the use of AI can simultaneously generate gains in productivity and work quality, but also risks associated with bias, confidentiality and work intensification (OECD, 2023a; Green, 2024). From a complementary perspective, the literature on digital transformation and sustainable entrepreneurship reinterprets economic risk as a "hybrid" phenomenon, in which the traditional vulnerabilities of small firms are amplified by risks endogenous to digitalization, such as cyber exposure, technological risk, the volatility of digital markets and the risk of organizational adaptation. This approach supports the argument of the paper by indicating the relevance of AI and ML not only as sources of efficiency, but also as mechanisms for managing uncertainty, with direct implications for the resilience and sustainability of digital transformation outcomes in SMEs (Chiriță, 2025).

In SMEs, where functions are often less specialized, this reconfiguration of skills can have disproportionate effects: it either accelerates "augmentation" (more with fewer resources) or amplifies risks through uncontrolled use, lack of internal standards and absence of validation mechanisms. Recent evidence on the participation of SMEs in competitive processes involving high administrative requirements shows that barriers frequently arise from procedural compliance difficulties, bureaucratic burden and limited internal capacity to manage documentation and associated workflows. In these conditions, the difference between firms

is not only caused by the intention of adopting technologies, but also by the ability to standardize processes, reduce errors and strengthen the organizational skills needed to meet compliance requirements. This perspective supports the argument of the article, as intelligent automation and ML can contribute to reducing operational friction by automating checks, assisting document preparation and increasing the quality of decisions, with an effect on the resilience and competitiveness of SMEs (Dobrotă, Sârbu, & Stanciu, 2022).

Given that comparable data at the firm or sector level on the integration of AI/ML in SMEs is frequently limited, fragmented or publicly inaccessible, this article proposes research based on a critical analysis of recent literature, thus pursuing three main objectives:

O1. Clarifying how intelligent automation and ML are integrated into the digital transformation practices of SMEs and identifying the implementation models outlined in recent literature (2024–2025, from point adoption in support functions, to end-to-end orchestration with governance).

O2. Highlighting how this integration influences exposure to emerging economic risks, either by reducing operational and financial vulnerabilities (e.g., error reduction, response times, resource optimization), or by the emergence of new risks (compliance, security, bias, supplier dependency).

O3. Identifying organizational conditions that make the difference between value generation and risk amplification, with a focus on data quality, skills, governance, auditability, and human-in-the-loop process design.

Through this structuring, the article contributes to the literature on the digital transformation of SMEs in two directions: (i) proposes an integrated reading of AI and ML as a unitary technological and organizational mechanism (not as separate initiatives), and (ii) explicitly introduces the economic risk-aware dimension in the assessment of AI adoption, treating emerging risks not only as a "context", but as a variable that conditions the implementation design, governance, and sustainability of benefits.

2. Literature review

In recent years, interest in the digitalization of SMEs has increased significantly, amid economic uncertainties, competitive pressures and the need to quickly adapt to volatile market conditions. The 2024–2025 literature treats the digital transformation of SMEs not only as a program of technological modernization, but as a process of reconfiguring operational models and organizational capabilities, in which AI/ML and automation become decision and coordination infrastructures (not just tools). In this vein, studies on the "digital divide" show that AI can contribute to either reducing or amplifying the gaps between firms, depending on access to resources, skills and digital ecosystems (Kergroach, 2025; Arroyabe et al., 2024).

A substantial body of policy analysis (notably OECD) argues that the benefits of AI for SMEs are conditional on complementary inputs (data, infrastructure, skills, change management) and the ability to integrate AI into core processes, not just peripheral activities. Recent taxonomies (such as "explorers/optimizers/champions") suggest a heterogeneous distribution of AI maturity in SMEs and indicate that perceived risks (accuracy, harmful content, legal uncertainty) remain significant barriers even for adopters (OECD, 2025a; OECD, 2025b).

Intelligent automation is conceptualized as the integration of RPA technologies with workflow automation tools and AI components, such as NLP, computer vision, generative models, for end-to-end automation and continuous process improvement. In this formula, RPA remains the execution layer (task automation), and AI/ML becomes the cognitive layer that allows for variation handling, content interpretation, and adaptation to operational contexts. Although some of the applied literature includes white papers, they converge in describing AI as a "bridge" between operational efficiency and analytical capabilities for decision-making (Ng et al., 2021; Patrício et al., 2025).

In SMEs, AI is frequently reported in administrative and support processes (back-office processes, documents, customer relations), because these processes are intensely repetitive, have relatively high coordination costs, and are often poorly standardized. However, the literature emphasizes that "automation" in SMEs has a strong process redesign component: value emerges when automations are aligned with strategic objectives (response time, quality, cash-flow), not when they are implemented as piecemeal initiatives (Le Dinh et al., 2025; Ng et al., 2021).

AI adoption is systematically influenced by existing digital infrastructure, technological literacy, data availability, and leadership capacity to support change. The 2024–2025 literature treats these conditions as "complementary capabilities": without them, AI can produce fragile automation that is difficult to maintain and has limited impact on performance. The OECD points out that SMEs face structural barriers related to data, skills, and financing, and that in practice, many implementations are vendor-dependent and "embedded" (integrated into applications) solutions, which can reduce control over operations and risks (OECD, 2025a;

OECD, 2025c). At the same time, the literature on SME digitalization proposes maturity frameworks (awareness–strategy–adoption–continuous improvement), which suggest that results are better when AI is implemented incrementally, with data governance, monitoring and organizational learning (including adjustment of roles and responsibilities) (Le Dinh et al., 2025; OECD, 2025a).

ML is analyzed as a key tool for extracting value from organizational data, with recurring applications in demand forecasting, anomaly detection, customer segmentation and supply chain optimization. The supply chain management literature confirms the role of AI/ML in improving visibility, prediction and resilience, but also emphasizes the dependence on data quality and cross-system integration (ERP/CRM/logistics) (Filippucci et al., 2024; Frank et al., 2019).

For SMEs, a robust finding is that ML is often accessed through commercial solutions (ERP/CRM/SaaS) that offer "AI-ready" functionalities, reducing the cost of entry, but increasing the risk of opacity (lack of transparency on training data, parameterization, boundaries) and the difficulty of auditing decisions. The OECD explicitly notes that SMEs report concerns about accuracy, risks of problematic content and legal uncertainty, indicating that the "decisional benefits" of ML are not perceived as automatic, but as dependent on control and governance (OECD, 2025a; OECD, 2025c; Le Dinh et al., 2025).

An important sub-current from 2024 to 2025 is the integration of GenAI (LLM, co-pilots, conversational assistants) into SMEs' processes: content generation and review, customer support, text analysis, document synthesis, assisted automation. The OECD explicitly analyses the effects of GenAI on the workforce in SMEs, identifying both the potential to compensate for skills and staff shortages and the main barriers: mismatch with the company's activity, copyright/legal concerns, confidentiality of data entered into models and lack of skills (Brynjolfsson et al., 2025; OECD, 2025b).

From the perspective of the AI literature, this GenAI wave has a "democratizing" effect (lower entry cost, natural interfaces), but also raises additional control issues: variable quality of results, hallucinations, confidentiality, intellectual property, plus dependency on suppliers (model lock-in). Thus, GenAI tends to accelerate adoption, but increases the need for validation mechanisms ("human-in-the-loop"), internal policies and monitoring tools (Rajaram & Tinguely, 2024; ISO/IEC, 2023).

A critical dimension in the recent literature is the assessment of emerging risks associated with AI/ML integration in SMEs. At the macro level, WEF reports describe a more fragmented and volatile global risk landscape (including geopolitical, technological and disinformation risks), with indirect effects on business continuity and the investment environment (WEF, 2025a). On the digital front, WEF sources on cybersecurity explicitly point to "cyber inequity" (differences in resilience between small and large organizations) and vulnerabilities related to supply chain interdependencies, relevant for SMEs operating as suppliers or relying on cloud services and third-party AI solutions (WEF, 2025b).

Consequently, the literature treats intelligent automation as ambivalent from a risk perspective: it can reduce errors and delays (through standardization and monitoring), but it can also increase the attack surface and exposure to incidents if implemented without controls (security, access, logging, vendor management) (WEF, 2025b; Tabassi, 2023; ISO/IEC, 2023). In the recent literature, ML risks are arbitrarily analyzed in terms of bias, transparency or auditability. A series of reviews that refer to algorithmic bias highlight the fact that distortions can occur throughout the life cycle, from the data, modeling, implementation or feedback perspective. At the same time, mitigation requires both technical tools and a series of organizational processes, such as validation, documentation or other responsibilities of this kind (Bankins et al., 2024; Milanez, 2025). Moreover, applied research shows the difficulty of audits in contexts where decision-making mechanisms are opaque (e.g., proprietary platforms or systems), which is particularly relevant for SMEs using "embedded" models in SaaS (Tabassi, 2023; ISO/IEC, 2023).

Therefore, the converging literature suggests that auditability in SMEs should be designed pragmatically: minimal traceability, performance and bias tests on critical cases, escalation procedures when predictions conflict with operational reality, and clear separation of responsibilities between provider and user. A cross-cutting theme is that the digital transformation driven by AI/ML is not only technological, but also one of skills, roles, and work organization. The literature on AI in the workplace highlights mixed effects on productivity and skill demand, suggesting that AI tends to increase the importance of digital and coordination/interpretation skills (OECD, 2023; Green, 2024; Babashahi et al., 2024).

In SMEs, where roles are more generalist, "AI literacy" becomes a multiplier: without understanding the boundaries (error, applicability conditions, confidentiality), the use of AI can amplify operational and legal risks. Recent literature converges in showing that AI and ML are important catalysts of digital transformation in SMEs, but their impact is strongly conditioned by integration into end-to-end processes, data quality and availability, internal skills and the existence of governance mechanisms. In this context, several gaps relevant

to the present research emerge. First, comparable evidence at the firm or sector level remains limited, as many studies are qualitative or focused on specific industries, which reduces the possibility of generalization. Second, the causal relationship between AI–ML adoption and resilience to economic risks is rarely measured explicitly. Although the benefits are frequently discussed, the effects on operational continuity, response times or flow stability are insufficiently quantified. Third, governance and compliance are often analyzed in a fragmented manner, with separate treatments for security, bias, audit and legal risk, although in real implementations these dimensions are interdependent. Finally, GenAI integration tends to accelerate adoption, but increases the complexity of control, amplifying the need for internal policies, monitoring and human-in-the-loop practices, especially in resource-constrained SMEs (OECD, 2025b). Therefore, the article argues that the assessment of AI–ML in SMEs should be carried out simultaneously from the perspective of value creation (efficiency and decision quality) and risk management (security, compliance, technological dependencies and quality), taking into account the structural constraints specific to small firms.

3. Bibliometric Mapping and Thematic Synthesis: Positioning Intelligent Automation and ML for Risk-Aware Digital Transformation in SMEs

We identify the need to introduce a systematic structuring stage of the field to reduce the risk of a fragmented reading (technological vs. managerial vs. risk) and to explicitly highlight how the dominant themes are linked to each other. Thus, bibliometric keyword co-occurrence mapping is used here as a tool to validate and consolidate the conclusions from the recent literature, providing an aggregated representation of how the scientific community connects in practice: ML/AI, SME digital transformation and emerging economic risks. On the logic of the article's premise, this section aims to show that intelligent automation and ML cannot be credibly analyzed separately: ML generates predictive and cognitive capabilities, and intelligent automation represents the orchestration layer that "translates" them into end-to-end results (time, cost, quality, control, resilience). Therefore, bibliometric mapping functions as a bridge between the conceptual review and the central argument of the article: SME digital transformation becomes "risk-aware" when ML is operationalized through intelligent automation in governed and auditable processes.

The mapping includes two complementary visualizations. The first is represented by Figure 1 (the co-occurrence network) highlighting the relational structure of the themes: nodes (keywords), links (co-occurrence), and clusters (thematic subdomains). The second is represented by Figure 2 (the density map) highlighting the salience of the themes, indicating the areas with the highest semantic concentration and, implicitly, the most “productive” or dominant areas in the recent literature. This combination of visualizations allows for both a structural reading, in the sense that we observe who connects with whom and through which themes, but at the same time an interesting reading.

Figure 1 highlights the intellectual structure of the field through a network of terms in which the size of the nodes suggests the salience of the topics, and the links reflect their co-occurrence in the same literature. The centrality of the machine learning and small and medium enterprise nodes shows that recent literature positions ML as a transversal “engine” of the digitalization of SMEs, not as a niche application. Around this core, thematic clusters are distinguished that exactly reflect the tension in the title of the paper: technology-guided digital transformation, under economic risk constraints.

The “risk & prediction” cluster (blue), terms such as bankruptcy prediction, credit risk, default prediction, financial ratios, failure prediction, indicate that a significant part of the research connects ML with the management of economic risks and the fragility of firms (insolvency, credit risk, performance degradation). The presence of this cluster confirms that “emerging economic risks” are not just a context, but a major application area in which ML is mobilized for anticipation and control.

The “management–innovation–digital transformation” cluster (green), terms such as management, innovation, digital transformation, capabilities, adoption, impact, suggest a literature oriented on organizational capabilities and effects: how technology is translated into performance and competitiveness, especially through digital maturity, resources and strategy. This cluster anchors the contribution of the article on the “drivers of digital transformation” issue.

The “deep learning / anomaly detection / optimization” cluster (red) highlights a technical core (algorithms, classification, anomaly detection) that fuels practical applications, but which risks remaining “disconnected” from organizational mechanisms if not integrated into end-to-end flows.

The “AI–Industry 4.0–cybersecurity–big data” area (yellow/purple) connects operational digitalization (Industry 4.0, IoT, smart manufacturing) with cybersecurity and big data, suggesting that digital transformation in SMEs occurs in interdependent technological ecosystems, where risk is both economic and digital (continuity, security, supplier dependencies).

In conclusion, Figure 1 suggests that the literature has evolved towards two strong, but often treated separately, directions: (i) ML for prediction and economic risk and (ii) ML/AI as a tool for managerial transformation. This is where the contribution of the article is positioned: intelligent automation as a mechanism for "putting into production" ML in end-to-end processes, transforming predictions into operational outcomes and measurable resilience.

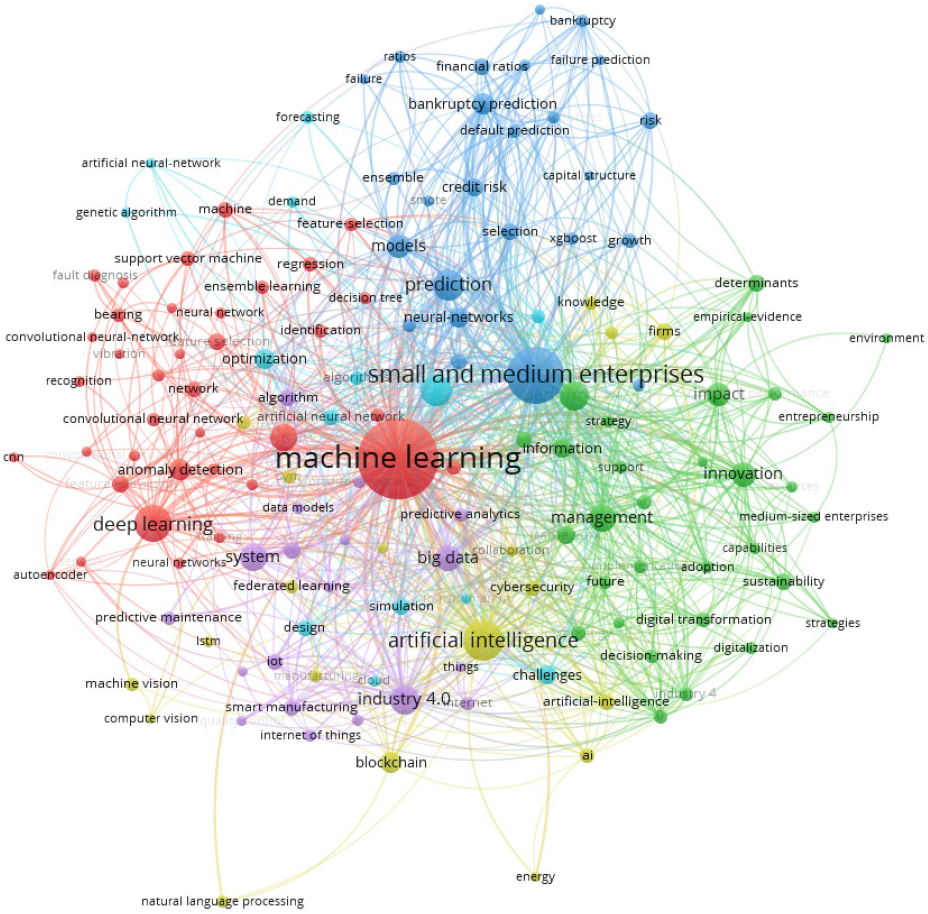

Figure 1. Co-occurrence network of keywords in the literature on ML/AI and SMEs (thematic map)

Source: created by the authors with VOSviewer, based on Web of Science Core Collection data, Clarivate (2025)

Figure 2 visually confirms, through density (the most intense areas), that the literature is dominated by the triad machine learning – SMEs – artificial intelligence, which reinforces the idea that ML and AI are perceived as central infrastructures for the digitalization of SMEs. Secondary densities are observed around the terms' prediction, deep learning, management, innovation, showing that there are two complementary development axes.

Also, the decisional/risk axis shows that ML is used intensively for prediction (including sub-risks such as bankruptcy prediction and credit risk), which supports the relevance of the "emerging economic risks" dimension in the title, in the sense that in a volatile environment, the value of technology is linked to anticipation, early detection of degradations and uncertainty management.

Regarding the organizational/transformation axis, this shows that the density around management and innovation may suggest that performance does not only depend on algorithms, but also on integration capabilities, governance and organizational change.

Although ML/AI are highly visible, the link between analytics and end-to-end execution is often implicit, and this becomes one of the elements debated in this article, namely intelligent automation (hyperautomation) as a layer that operationalizes ML in workflows, controls and auditability, i.e. the exact mechanism by which SMEs can transform AI from "potential" into economic resilience and competitive advantage, without amplifying new risks (compliance, security, technological dependence).

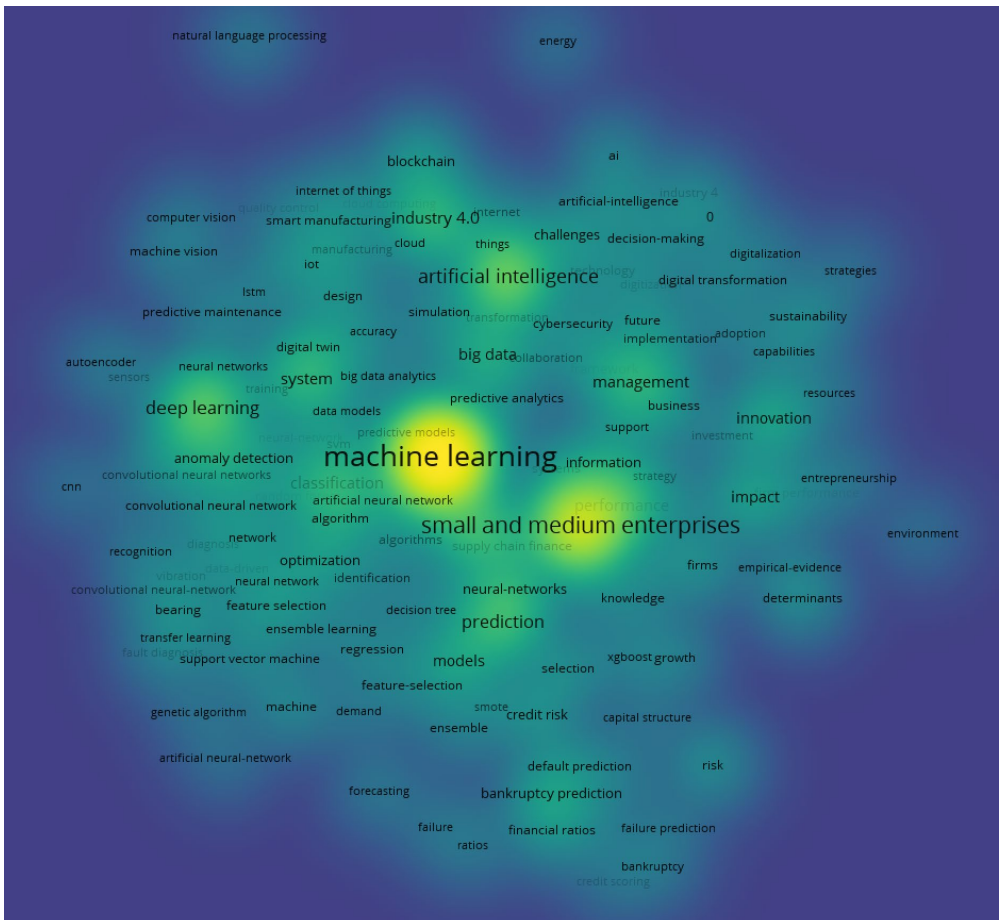

Figure 2. Topic density map: topic salience and concentration

Source: created by the authors with VOSviewer, based on Web of Science Core Collection data, Clarivate (2025)

Thematic mapping shows that recent literature is strongly focused on ML/AI in SMEs and on the use of prediction in risk contexts (insolvency, credit, performance). However, the organizational mechanism by which ML has observable economic impact under conditions of uncertainty remains insufficiently clarified: integration into processes, governance, controls and skills. This is where the contribution of this article fits in, treating intelligent automation and ML as an integrated system for "risk-aware" digital transformation, identifying the conditions in which adoption produces value versus amplifies vulnerabilities.

Based on the structure and thematic density, an interpretation framework is outlined in which the digital transformation of SMEs (outcome) is the product of the interaction between three sets of conditions.

The first set of conditions refers to technological capabilities (ML/AI), i.e. predictive or cognitive models, advanced analytics, content generation, or anomaly detection.

The second set of conditions considers implementation capabilities, called intelligent automation, which relate to integration in end-to-end flows, orchestration, monitoring, control, and operational standardization.

And the third set of conditions highlights those organizational capabilities (governance & skills), which relate to data quality, competencies (AI literacy), leadership, change management, or security and compliance policies.

Through this integration, the article highlights and argues that ML/AI represents the "cognitive engine", and intelligent automation represents the "transmission" that converts cognitive potential into economic results and resilience. In the absence of the implementation and governance layer, ML often remains a "pilot" or "isolated functionality", and the effect on emerging economic risks is limited and potentially volatile.

The results of the thematic mapping indicate four relevant gaps, directly aligned with the importance of the research:

L1. Fragmentation between "ML for prediction" and "digital transformation as organizational change": the literature covers both, but often without explaining the operational mechanism that unites them. Insufficient clarification of the role of intelligent automation as an infrastructure for operationalizing ML: ML applications and benefits are discussed, but the end-to-end orchestration, control and audit layer is less often analyzed.

L2. Risk management as an emergent outcome, not as a design object: risks are frequently listed, but less integrated into the implementation architecture (controls, policies, validation).

L3. Technological dependencies and governance in SMEs: embedded/SaaS solutions reduce entry barriers, but increase opacity and operational accountability issues.

Consequently, the article can be guided by the following research questions (RQ), consistent with the objectives in the introduction:

- ✧ RQ1: How is ML integrated into intelligent automation initiatives in SMEs, so that end-to-end results are observed and not just point-by-point automation?
- ✧ RQ2: To what extent would this integration reduce vulnerabilities associated with emerging economic risks, referring here to demand volatility, cost pressures, supply chain disruptions, capital constraints?
- ✧ RQ3: What new risks arise from the integration of ML into automation, referring to bias, systemic errors, security, compliance, supplier dependencies and how can these be governed proportionately in SMEs?
- ✧ RQ4: To what extent and through what mechanisms, such as data quality, skills, Human-in-the-Loop systems, monitoring and auditability or organizational conditions specific to SMEs, does the outcome of AI/ML adoption differ, when we talk about value creation or amplification of operational and strategic risk?

Thus, through thematic mapping, we have demonstrated that the 2024–2025 literature is strongly focused on ML/AI in SMEs and that a significant part of the field connects these technologies with the prediction and control of economic risks. At the same time, the analysis highlights a structural gap: the lack of a sufficiently robust explanation of the mechanism by which ML capabilities are transformed into operational results and economic resilience in SMEs.

In this gap, the contribution of the article is inserted: the conceptualization of intelligent automation and ML as an "integrated system" of digital transformation in SMEs, in which the automation layer is not an accessory, but a condition of impact and a governance mechanism in an environment marked by emerging economic risks. The following chapters can develop this argumentation through: implementation typologies, value creation mechanisms, risk profiles and recommendations for management and public policies.

4. Conceptual Framework and Implementation Typologies for Risk-Aware IA–ML Adoption in SMEs

The literature summarized in the previous chapters, supported by the thematic mapping of the 2024–2025 corpus, indicates a strong convergence around the machine learning–artificial intelligence–SMEs triad and a consistent focus on prediction applications associated with economic risk (insolvency, credit risk, failure, volatility). This thematic structure suggests that ML/AI are increasingly treated as infrastructures for decision and competitiveness, but also highlights an analytical fragmentation: some studies remain anchored in technical discussions about models and performance, others in managerial frameworks about adoption and capabilities, and a third in risk inventories without sufficient explanation of the mechanism through which these dimensions are integrated into end-to-end results. OECD reports on AI adoption in SMEs explicitly emphasize that benefits do not occur automatically, being conditioned by complementary inputs such as data, skills, governance and integration into processes, while WEF analyses on risks and security indicate disproportionate vulnerabilities for small organizations in contexts of increased digital interdependencies (OECD, 2023; OECD, 2025; WEF, 2025).

Within this framework, the article is guided by four research questions consistent with the objectives of the introduction: integrating ML into intelligent automation initiatives to generate end-to-end results (RQ1), the contribution of this integration to reducing vulnerabilities associated with emerging economic risks (RQ2), the emergence of new or amplified risks through the integration of ML into automation and the conditions for proportionate governance in SMEs (RQ3), respectively identifying organizational conditions that differentiate between value generation and risk amplification (RQ4).

Consistent with these questions, the chapter proposes a "risk-aware" conceptual framework in which risk is not treated as an exogenous variable, but as a factor that shapes the design of the implementation, including the selection of automated processes, the level of autonomy, control mechanisms, and governance architecture. This positioning is compatible with the recent literature on integrating AI into processes, which emphasizes that value results from coupling operational efficiency with data-driven decision-making and monitoring and auditability mechanisms, not just from one-off or mimetic implementations (OECD, 2025; Callari & Puppione, 2025).

4.1. Defining key constructs and their relationships

In this article, intelligent automation (intelligent automation/hyperautomation) is conceptualized as an end-to-end automation architecture that combines the task execution layer (RPA and workflow automation)

with cognitive capabilities (ML, NLP, computer vision and generative tools), integrated into a system of orchestration, monitoring and continuous improvement. This definition reflects the evolution from rigid automation to adaptive automation, capable of managing variation and unstructured content, but also supporting traceability and decision control. Machine learning (ML) is treated as a cognitive engine that produces decision signals through prediction, classification, recommendation and anomaly detection, extending automation beyond deterministic rules and enabling probabilistic decisions, especially relevant in volatile environments.

Emerging economic risks are defined as sources of uncertainty and shocks that directly affect the performance of SMEs, including demand volatility, cost pressures, supply chain disruptions, capital constraints and regulatory uncertainties. In parallel, digital/AI risks are conceptualized as risks endogenous to the digitalization process, such as cybersecurity and privacy, decision bias and opacity, performance degradation through drift and technological dependencies on suppliers and platforms. The OECD explicitly addresses the risks perceived by SMEs in using AI (from accuracy and lack of skills to legal and privacy risks), and the literature on governance and auditability emphasizes that integrating AI into operational decisions requires accountability and traceability mechanisms that go beyond the "pilot" level (OECD, 2025; Cowgill et al., 2024).

The relationships between the constructs are formulated in functional terms. ML generates decision signals, but the economic impact only occurs if these signals are operationalized in processes. In the proposed framework, the basic relationships are:

(i) ML → (decision signals) predictions/recommendations/anomalies;

(ii) AI → (execution mechanism) integration into processes + control + auditability;

(iii) Organizational capabilities (data, skills, governance) → condition the transformation of ML signals into results;

(iv) Emerging risks → increase the value of the prediction, but also increase the cost of error; therefore, they impose a "risk-aware" design.

Intelligent automation is the execution and integration mechanism that connects ML predictions and recommendations to end-to-end flows, including control rules, logging mechanisms and auditability. In this chain, organizational capabilities, especially data quality and governance, skills and AI literacy, as well as governance architecture and supplier management, condition the transformation of ML signals into observable results. Emerging risks increase the value of prediction and automation, but also amplify the cost of error, which justifies a proportional "risk-aware" design, in which the autonomy of the system is calibrated according to the criticality of decisions and the control capacity (OECD, 2023; OECD, 2025; WEF, 2025).

4.2. Proposed Conceptual Framework: Capabilities, Mediators, and Outcomes Under Risk

The proposed conceptual framework explains the digital transformation of SMEs as a causal chain in which AI–ML capabilities generate value only when supported by organizational mediators and integrated into appropriate governance. Essentially, ML produces capabilities for anticipating and interpreting context (e.g., forecasting, prioritizing, anomaly detection), and intelligent automation transforms these capabilities into actions integrated into end-to-end processes (e.g., triage, allocation, escalation, execution, and monitoring). However, the performance and robustness of this chain are mediated by four organizational conditions recurring in recent literature, namely data quality and availability, skills and AI literacy, governance mechanisms (accountability, control, audit, compliance), and technology management of suppliers, including security and privacy.

In addition, emerging economic risks act as a moderator of the relationship between adoption and outcomes. In unstable environments, the pressure for speed and adaptation increases, which amplifies the value potential of AI–ML. At the same time, volatility makes models more exposed to drift and automations become more fragile if they do not include fallback mechanisms, monitoring and human intervention. This double-edged sword effect explains why the literature insists on governance and skills as differentiating factors between value-creating and risk-amplifying scenarios, especially in SMEs operating with limited resources and with greater dependence on integrated commercial solutions (OECD, 2025; WEF, 2025; Callari & Puppione, 2025).

The conceptual framework therefore serves as a basis for the implementation of typologies and for the analysis of value-creating and control mechanisms, developed in the following chapters, directly answering questions RQ1–RQ4. Figure 3 summarizes the conceptual framework of the paper in a horizontal representation, which emphasizes the sequential and end-to-end nature of AI–ML-based digital transformation in SMEs, under the pressure of emerging economic risks. The horizontal organization has a clear analytical role: it makes visible the fact that AI–ML produces value only when the entire logical chain is followed, from the initial conditions and contextual constraints to the results and organizational learning. Consequently, the figure does not function as a

simple descriptive scheme, but as a framework for interpreting the mechanisms through which technology becomes economic performance and resilience.

In the Context segment, the figure positions the initial environment and the specific constraints of SMEs as the starting point for adoption. These include demand volatility, cost pressures, supply chain dysfunctions, limited access to capital, and regulatory uncertainty. As inputs, they increase both the utility of prediction and automation and the cost of error, justifying an explicitly "risk-aware" approach to solution design. The next segment, Technical Capabilities, captures the AI–ML "package" through which the organization tries to respond to these pressures. In functional terms, ML provides cognitive capabilities (prediction, recommendation, anomaly detection, including NLP/GenAI), and intelligent automation operationalizes these capabilities in end-to-end processes through integration, orchestration, and monitoring, reducing execution times and operational variability.

The transition to Organizational Mediators is essential and is well highlighted by the horizontal flow. The figure highlights that the relationship between capabilities and outcomes is mediated by organizational conditions such as data readiness, skills and AI literacy, governance, as well as vendor and security management. These elements simultaneously condition performance and risk control, as they determine the quality of inputs, the calibration of automated decisions, auditability and robustness of implementation. In their absence, AI–ML can produce fragile automation, systemic errors or compliance and security vulnerabilities.

The Outcomes segment groups the expected economic and organizational results, treated multidimensionally, referring to: operational efficiency, decision quality, resilience, strengthening compliance and trust through control mechanisms for the SME context.

Finally, the Feedback Loop emphasizes the dynamic nature of AI–ML adoption and justifies the horizontal representation as a "cycle" of improvement, that is: monitoring performance and drift, learning from results and recalibrating policies and processes are necessary to maintain value in volatile environments but also to prevent model degradation or amplification of vulnerabilities.

Figure 3. Conceptual framework linking IA–ML capabilities, organizational enablers, and outcomes under emerging economic risks

Source: Authors' elaboration based on the reviewed literature and thematic synthesis

Thus, Figure 3 operationalizes the central argument of the article: AI and ML become drivers of "risk-aware" digital transformation in SMEs only when implemented as an integrated end-to-end system, supported by organizational mediators and governance, and maintained through continuous monitoring and improvement mechanisms.

4.3. Typologies of AI–ML implementation in SMEs: from "quick wins" to end-to-end orchestration

Based on the literature from 2024 to 2025 and the thematic logic highlighted through mapping, four dominant typologies of AI–ML implementation in SMEs are outlined, which can coexist in the same organization depending on digital maturity and economic risk pressure. These typologies are relevant to the contribution of the paper because they explain the difference between adoptions that produce quick but fragile benefits, and adoptions that generate resilience and competitive advantage, but require adequate governance, skills, and data. In relation to the title of the study, the typologies function as a bridge between technology and "risk-aware" outcomes, showing that the impact of AI–ML depends on the level of integration into processes and the ability of SMEs to control the newly introduced risks.

The first typology is oriented towards task automation and back-office efficiency, centered on RPA and workflow automation, with low or moderate use of ML. In this form, SMEs mainly aim to reduce costs and errors in repetitive activities, such as invoicing, reconciliation, database updates, reporting or document processing. ML usually appears on a one-off basis, for example, for document classification or extracting fields from forms. The value is quickly observable, but remains vulnerable to the fragility of rule-based automation and the lack

of process standardization. In the absence of monitoring and exception mechanisms, these implementations can become "brittle", with benefits eroding in volatile contexts.

The second typology focuses on augmented analytics and decision support, with ML as the main element and a limited level of operational orchestration. In this configuration, SMEs use ML for forecasting and recommendation, especially for demand, inventory, customer segmentation, anomaly detection or default risk estimation. This typology has high potential in conditions of uncertainty, as it promises to reduce decisional "blindness" and improve resource allocation. However, the risk increases when predictions remain "outside the process", that is, they are not integrated into flows with validation, responsibilities and acceptance criteria. In such cases, drift, data errors and bias can lead to wrong decisions, and anticipated benefits can turn into operational volatility.

The third typology, which is also the most consistent with the central argument of the paper, aims at intelligent end-to-end automation or hyperautomation, through the tight integration of AI and ML. Here, ML signals are embedded directly into complete operational flows, from sorting and automatic allocation to approvals, logging, monitoring and escalation, so that predictions become observable actions and economic outcomes. In this configuration, AI is not an auxiliary technical layer, but the mechanism that operationalizes ML in governed processes, making it possible to both increase efficiency and strengthen resilience in the face of emerging economic risks. This is precisely why this typology expresses the logic of the title most clearly: AI and ML become drivers of digital transformation under risk when orchestrated end-to-end, with proportionate controls, monitoring and auditability.

The fourth typology is oriented towards GenAI-based front-office automation, with direct interaction with customers and a greater need for governance. This includes conversational assistants, content generation and personalization, customer support, sales and marketing or rapid feedback analysis. The benefits are mainly related to scalability and speed, which are attractive for SMEs in resource-constrained contexts. However, this typology brings sensitive risks, such as quality variation, data confidentiality, intellectual property, compliance and reputational risk. In the absence of clear usage policies, human validation in critical cases and data protection measures, GenAI can amplify vulnerabilities precisely in areas with maximum public exposure.

Overall, the four typologies suggest that the transition from quick wins to sustainable impact depends on moving from ad hoc uses to end-to-end integration, as well as on the development of organizational mediators. They support the conclusion that risk-aware digital transformation in SMEs is not only driven by the adoption of AI–ML, but by how these technologies are implemented as an integrated system, with appropriate governance, skills, and control of emerging risks and those introduced by automation.

In the recent literature, as seen in Table 1, a coherent set of mechanisms emerges through which AI–ML can generate value in SMEs under emerging economic risks, especially in contexts of volatility, when pressures on reaction time and efficiency are accentuated.

A first mechanism is the reduction of operational friction, as end-to-end automation decreases delays, errors and coordination costs, which contributes to stabilizing cash flows and increasing the predictability of delivery.

Table 1. IA–ML implementation archetypes in SMEs and expected value/risk profiles SMEs

No.	Domain	Barrier / Risk Factor	Implications under emerging economic risks	Mitigation mechanism / organizational enabler	Representative sources
1	Data readiness	Low data quality, fragmentation, limited interoperability	Weak model performance and unreliable automation; delayed decisions during demand shocks; limited ability to reconfigure processes end-to-end.	Data governance (ownership, quality rules), minimum viable data model, integration via APIs/ETL, metadata and logging for auditability.	(OECD, 2025a; Le Dinh et al., 2025)
2	Financial capacity	Limited investment budgets and uncertain ROI	Postponed or "piecemeal" adoption; underinvestment in security/monitoring; higher vulnerability to cost pressures and capital constraints.	Phased adoption (use-case prioritization), shared services/consortia, public support schemes; KPI-based business cases for scaling.	(OECD, 2025a; Haq et al., 2025)

No.	Domain	Barrier / Risk Factor	Implications under emerging economic risks	Mitigation mechanism / organizational enabler	Representative sources
3	Skills & AI literacy	Skills gaps (AI literacy, data skills, process design) and limited managerial bandwidth	Higher probability of mis-specifying use cases and over-trusting outputs; reduced resilience when models/automation fail or drift.	Targeted upskilling, role redesign (human-in-the-loop), internal "AI champions", structured training for prompt/validation and data interpretation.	(OECD, 2025b; Le Dinh et al., 2025)
4	Governance & accountability	Lack of policies for model validation, explainability, oversight and responsibility	Compliance risk under evolving regulation; reputational loss in case of biased or unsafe automated decisions; limited trust from customers and partners.	AI governance framework (risk classification, documentation, approvals), audit trails, model cards, escalation procedures.	(European Union, 2024; ISO/IEC, 2023)
5	Cybersecurity & privacy	Expanded attack surface and sensitive data exposure through integration (RPA + ML + SaaS)	Higher likelihood of disruption, fraud, or data leakage; increased operational risk in supply-chain dependent ecosystems.	Security-by-design (access control, encryption, secrets management), vendor security assessments, incident response, continuous monitoring.	(World Economic Forum, 2025b; Tabassi, 2023)
6	Vendor dependence	Vendor lock-in and limited transparency of embedded AI in SaaS/ERP platforms	Reduced control over model behavior and updates; dependency risk under price changes or service outages; limited ability to meet audit demands.	Contractual safeguards (SLA, portability, transparency), multi-vendor strategy, preference for interoperable components and open standards.	(OECD, 2025a; Le Dinh et al., 2025)
7	Model risk & drift	Model drift, concept drift, and automation errors in volatile environments	Forecasting errors during demand volatility; inventory or credit decisions deteriorate; cascading failures across automated workflows.	MLOps/ModelOps (monitoring, retraining triggers), back-testing and stress tests, guardrails and fallbacks to manual review.	(Tabassi, 2023; OECD, 2025a)
8	Organizational change	Resistance to change and low trust in automation/AI recommendations	Slow adoption and underutilization; risk of "shadow AI" practices; reduced coordination capacity during disruptions.	Change management, participatory design, transparency about limitations, incremental rollout with feedback loops.	(OECD, 2025b; Haq et al., 2025)
9	Strategic alignment	Misalignment between IA–ML initiatives and business strategy	Technology-led pilots that do not scale; limited impact on resilience, competitiveness and productivity under shocks.	Strategic roadmap linking IA–ML to measurable outcomes; portfolio governance; prioritization based on risk exposure and value.	(OECD, 2025a; Haq et al., 2025)
10	Measurement & value realization	Insufficient metrics for value, risk, and compliance performance	Inability to demonstrate benefits; uncontrolled risk accumulation; difficulty justifying continued investment.	Balanced KPI set (efficiency, decision quality, risk/compliance), periodic reviews, continuous improvement loops.	(Le Dinh et al., 2025; ISO/IEC, 2023)

Note. IA = intelligent automation; ML = machine learning; SMEs = small and medium-sized enterprises. The table synthesizes recurring themes in recent evidence and the reviewed literature

Source: Authors' elaboration based on the reviewed literature and thematic synthesis

A second mechanism is related to anticipation and rapid response, as ML improves forecasting capacity and early detection of degradations in demand, inventories or non-payment risk, reducing the cost of surprises and allowing proactive interventions.

A third mechanism considers resource reallocation, in the sense that intelligent automation frees up human time from repetitive activities, moving it towards the management of value-added activities, which is a critical aspect in SMEs affected by staff and skills constraints.

A fourth mechanism concerns organizational learning, because the feedback generated by monitoring and continuous improvement creates adaptive routines, useful for quickly recalibrating processes and decisions in an unstable environment.

At the same time, the literature emphasizes that the same technologies can produce mechanisms of risk amplification when the implementation is not adequately governed. A major risk is the emergence of systemic errors and drift, a situation in which initially performing models become inadequate as the economic environment changes, and automated decisions can transmit cascading errors in operational processes. A second risk is decisional opacity and bias, as automated decisions that are difficult to explain can harm customers or employees and increase legal and reputational risks, especially in sensitive areas such as lending, selection or customer relations. A third risk is vendor dependency, especially in the case of embedded or SaaS solutions, which can limit control over data and how models operate, reducing SMEs' ability to audit and intervene. A fourth risk is security and privacy, as end-to-end integration of AI–ML expands the attack surface and increases the likelihood of data exposure or incidents with operational impact.

These tensions explicitly justify a "risk-aware" approach, as positive outcomes do not only derive from adoption, but from calibrating the level of automation autonomy according to the criticality of the process and the cost of error. In practice, this calibration involves combining automation with human oversight mechanisms where the impact is high, continuous monitoring of performance and drift, and the introduction of governance, security, and auditability controls that make the use of AI–ML sustainable in conditions of emerging economic risk.

5. Risk-aware Value Creation and Control Mechanisms in SMEs: From Use Cases to Governance

The adoption of AI–ML technologies in small and medium-sized enterprises (SMEs) takes place in a context characterized by economic uncertainty and increased competitive pressures. In these conditions, digital transformation becomes a balancing act between value creation and risk management. Therefore, the implementation of AI–ML should be viewed not only as a technological innovation, but as a strategy to reduce organizational vulnerabilities. Demand volatility, rising costs, supply chain disruptions, limited access to capital, and regulatory changes are factors that determine the need for a "risk-aware" approach.

Recent literature highlights that the benefits of AI–ML depend on the degree to which these technologies are integrated into decision-making and operational processes. Also, SMEs that manage to connect prediction with automation and control can gain competitive advantages by reducing reaction times but also increasing resilience. Machine learning models can anticipate a series of demand variations, identify anomalies in data flows or assess the risk of non-payment. Intelligent automation, on the other hand, allows the implementation of these predictions in end-to-end processes, ensuring traceability, monitoring and rapid response capacity (Ng et al., 2021; Patrício et al., 2025; World Economic Forum, 2025a; OECD, 2025a).

However, the value generated by AI–ML is directly proportional to the degree of control over the risks introduced. Prediction models can degrade over time, algorithms can reflect biases, and integrated systems can generate technological dependencies or security vulnerabilities. In this sense, "risk-aware value creation" requires a balanced architecture between technological autonomy and human oversight. SMEs must adopt proportionate control mechanisms, adapted to the level of complexity and available resources.

Control mechanisms can be technical, process or organizational. At the technical level, it is essential to monitor data quality, verify model derivation and use drift detection mechanisms. At the process level, validation of automated decisions and traceability of results become minimum governance conditions. At the organizational level, control is achieved through clear responsibilities, AI governance policies, supplier management and the implementation of proportionate cybersecurity measures.

An effective governance framework for SMEs should not be bureaucratic, but "minimum viable." It includes a risk hierarchy, a risk register for each AI–ML project, a set of mandatory controls (data, skills, human validation, security), and operational and risk performance indicators. This type of governance ensures coherence between efficiency objectives and compliance requirements, reducing the risk of systemic failure or decision errors.

Table 2 also functions as an implementation design tool, as it operationalizes the principle of proportionality: the greater the impact of the process and the cost of error, the greater the need for human-in-the-loop controls, traceability, and drift monitoring.

Furthermore, the inclusion of monitoring indicators explicitly separates performance outcomes (value KPIs, such as time, cost, accuracy, and continuity) from risk indicators (risk KPIs, such as override rates, incidents, false alerts, policy violations), suggesting that the success of AI–ML in SMEs should be assessed simultaneously by efficiency and robustness. In this logic, the matrix can guide both the selection of high-yield use cases in

volatile contexts and the configuration of a "minimum viable governance" that allows for responsible scaling of automation without amplifying operational, security or compliance vulnerabilities.

Table 2. Emerging economic risks, IA–ML mitigation use cases, introduced risks, and recommended controls (SMEs)

Emerging risk (SME exposure)	IA–ML mitigation use cases (examples)	New / amplified risks introduced by IA–ML	Risk-aware controls (proportional for SMEs)	Monitoring indicators (value + risk KPIs)	Representative sources
Demand volatility (sales fluctuations, forecasting error)	ML demand forecasting; GenAI-assisted sales insights; IA-driven reorder automation	Drift during shocks; over-automation of replenishment; cascading inventory errors	Human approval thresholds for large orders; drift monitoring; scenario stress tests; fallback rules	Forecast error (MAPE), stockouts, excess inventory days; override rate	OECD (2025); Huang (2024); Brynjolfsson et al. (2025)
Cost pressures (energy, inputs, labor)	ML cost-to-serve analytics; optimization of scheduling and pricing; IA for invoice processing	Optimization bias; "local optimum" decisions; quality reduction	Policy constraints (min service levels); periodic review; explainability notes for pricing/scheduling	Margin variance; cost-to-serve; customer churn; exception rate	OECD (2023); Frank et al. (2019); Bankins et al. (2024)
Supply chain disruptions (delays, shortages)	Supplier risk scoring; anomaly detection on lead times; IA exception workflows in procurement	Data gaps across partners; false alarms; vendor dependency for data feeds	Data validation; multi-source signals; playbooks for exceptions; supplier diversification rules	OTIF (on-time-in-full); lead-time variance; alert precision; time-to-resolve exceptions	WEF (2025); Sarala et al. (2025); OECD (2025)
Limited access to capital / credit (cash-flow fragility)	ML cash-flow forecasting; receivables risk scoring; IA collections workflows	Biased credit decisions; compliance issues; feedback loops harming customers	Human-in-the-loop for adverse decisions; audit logs; fairness checks; documented decision criteria	DSO (days sales outstanding); bad debt rate; adverse decision review rate	OECD (2025); Cowgill et al. (2024); Milanez et al. (2025)
Regulatory uncertainty (AI, privacy, sector rules)	Compliance triage; IA for documentation and traceability; GenAI policy assistants	Non-compliant outputs; weak documentation; unclear accountability	Compliance-by-design checklist; model cards / usage policies; approval gates for changes	Audit findings; policy violations; traceability completeness; incident response time	European Union (2024); OECD (2025); Callari & Puppione (2025)
Cybersecurity and data breaches (increased integration surface)	ML anomaly detection for security events; IA incident response workflows; access automation	Larger attack surface; data leakage via GenAI; third-party vulnerabilities	Least privilege; encryption; prompt/data redaction; vendor security due diligence; backups	Security incidents; mean time to detect/respond; data access anomalies	WEF (2025); Sarala et al. (2025); OECD (2025)
Skills shortages (limited AI literacy, thin teams)	GenAI copilots for drafting/analysis; IA for routine tasks; ML decision support	Over-reliance; "automation bias"; unvalidated outputs	Training + AI literacy; mandatory review in critical workflows; usage guidelines	Review/override rate; error rate in outputs; training completion	OECD (2025); Brynjolfsson et al. (2025)
Vendor lock-in / platform dependency (SaaS embedded AI)	Embedded ML in ERP/CRM; IA via vendor automation suites	Opacity; limited auditability; data portability risk	Contract clauses (data export, SLAs); vendor risk assessment; modular architecture	Vendor downtime; portability tests; model transparency score	OECD (2025); Cowgill et al. (2024)

Note: SMEs can apply the matrix by (1) ranking risks by business impact, (2) selecting 2–3 high-leverage use cases, and (3) adopting the minimum viable control set for the risk level.

Source: Authors' elaboration based on the reviewed literature and thematic synthesis

Table 2 provides a summary of the main emerging economic risks for SMEs and how they can be managed through AI–ML technologies. The matrix highlights the correspondences between risk types, AI–ML

use cases, newly introduced risks and recommended control mechanisms. It provides a practical view of how AI–ML-based digital transformation can become a source of sustainable value when implemented in a risk-aware manner and properly governed. It is therefore emphasized that the success of SME digital transformation depends on the balance between innovation and control. AI–ML models can enhance efficiency and responsiveness, but without adequate controls they can generate operational and financial vulnerabilities. Integrating the risk-aware principle into the design, implementation and monitoring processes of AI–ML systems is the fundamental condition for a sustainable and responsible digital transformation.

6. Conclusions

This article has analyzed how intelligent automation (AI) and machine learning (ML) function as key enablers of digital transformation in SMEs, in a context dominated by emerging economic risks. Thematic mapping and critical synthesis of the 2024–2025 literature confirms that research is strongly focused on ML/AI in SMEs and on predictive applications associated with risk (insolvency, credit, financial fragility), but also highlights a major gap: the mechanism by which ML capabilities are transformed into end-to-end operational outcomes and economic resilience often remains insufficiently explained.

In relation to O1, the results show that AI–ML integration follows a continuum of maturity, from point adoptions in support functions, to end-to-end orchestration (hyperautomation) with monitoring and governance. The identified typologies explain why "quick wins" can be effective but fragile, while integrating AI+ML into complete flows is most compatible with digital transformation as an organizational change and with the theme of the article. The central contribution is the conceptualization of AI and ML as an integrated system: ML generates decision-making signals, and AI operationalizes them in controlled, auditable and monitorable processes.

In relation to O2, the analysis shows that AI–ML reduces vulnerabilities by reducing errors, accelerating response times, optimizing resources and increasing the ability to anticipate in volatile conditions. At the same time, AI–ML can introduce new or amplified risks, especially related to compliance, security, bias, drift and vendor dependency. Therefore, the benefits are not automatic, but dependent on the design of the implementation and proportional controls.

In relation to O3, the difference between "value" and "risk amplification" is determined by a coherent set of organizational conditions: data quality and governance, skills and AI literacy, human-in-the-loop mechanisms, auditability and supplier and security management. In an unstable environment, these elements are not optional, but become the minimum infrastructure for responsible scaling of automation and for maintaining performance over time.

Overall, the article contributes to two impactful ideas. The first is to treat AI–ML as an integrated sociotechnical mechanism, oriented towards end-to-end results, not as separate initiatives. The second is the explicit introduction of the "economic risk-aware" perspective, in which emerging risks condition the selection of use cases, the level of autonomy, governance and sustainability of benefits.

Based on the identified gaps and the proposed framework, the literature naturally opens up a series of topics of interest for future research, oriented both towards empirical validation and towards strengthening the applicative dimension. In particular, investigations into the differences in performance and resilience associated with different AI–ML implementation modes become relevant, as well as the development of "minimum viable" governance approaches adapted to the constraints of SMEs, including monitoring, auditability and proportional control. At the same time, it is worth delving deeper into the implications of technological dependencies in the case of embedded/SaaS solutions, including transparency, data portability and the risk of lock-in, along with the effects of GenAI on productivity and on reputational and compliance risks in scenarios with different degrees of human oversight. Finally, a cross-cutting area remains the analysis of the role of skills and AI literacy as determinants of implementation robustness, with a focus on the link between organizational maturity and the likelihood of systemic errors, drift or compliance incidents.

The final conclusion is that AI and ML can accelerate the digital transformation of SMEs and increase resilience to emerging economic risks, but only when they are integrated end-to-end, supported by data and skills, and governed by control and monitoring mechanisms. In the absence of this "risk-aware" design, AI adoption risks remaining superficial, fragile, and amplifying vulnerabilities precisely at moments of maximum volatility.

References

1. *Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Analyzing AI adoption in European SMEs: A study of digital capabilities, innovation, and external environment. Technology in Society, 79, 102733. https://doi.org/10.1016/j.techsoc.2024.102733*

2. *Babashahi, L., Barbosa, C. E., Lima, Y., Lyra, A., Salazar, H., Argôlo, M., Almeida, M. A. de, & Souza, J. M. de. (2024). AI in the workplace: A systematic review of skill transformation in the industry. Administrative Sciences, 14(6), 127. https://doi.org/10.3390/admsci14060127*
3. *Bankins, S., Hu, X., & Yuan, Y. (2024). Artificial intelligence, workers, and future of work skills. Current Opinion in Psychology, 58, 101828. https://doi.org/10.1016/j.copsyc.2024.101828*
4. *Bankins, S., Ocampo, A. C. G., Marrone, M., Restubog, S. L. D., & Woo, S. E. (2024). A multilevel review of artificial intelligence in organizations: Implications for organizational behavior research and practice. Journal of Organizational Behavior, 45(2), 159–182. https://doi.org/10.1002/job.2735*
5. *Brynjolfsson, E., Li, D., & Raymond, L. (2025). Generative AI at work. The Quarterly Journal of Economics, 140(2), 889–942. https://doi.org/10.1093/qje/qjae044*
6. *Callari, T. C., & Puppione, L. (2025). Can generative artificial intelligence productivity tools support workplace learning? A qualitative study on employee perceptions in a multinational corporation. Journal of Workplace Learning, 37(3), 266–283. https://doi.org/10.1108/JWL-11-2024-0258*
7. *Chiriță, M., & Sarpe, D.-A. (2025). Rethinking economic risk in the age of digital transformation and sustainable entrepreneurship. Annals of Dunarea de Jos University. Fascicle I: Economics and Applied Informatics, 31(2), 128–133. https://doi.org/10.35219/eai15840409519*
8. *Clarivate. (2025). Web of Science Core Collection [Database]. https://www.webofscience.com*
9. *Dobrotă, E. M., Sârbu, R., & Stanciu, S. (2022). The SMEs accessibility to public procurement in Romania: The grounds for bids rejection. Annals of Dunarea de Jos University of Galati, Fascicle I: Economics and Applied Informatics, 28(2), 68–75. https://doi.org/10.35219/eai15840409269*
10. *European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng*
11. *Filippucci, F., Gal, P., Jona-Lasinio, C., Leandro, A., & Nicoletti, G. (2024). The impact of artificial intelligence on productivity, distribution and growth: Key mechanisms, initial evidence and policy challenges (OECD Artificial Intelligence Papers No. 15). OECD Publishing. https://doi.org/10.1787/8d900037-en*
12. *Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. International Journal of Production Economics, 210, 15–26.*
13. *Green, A. (2024). Artificial intelligence and the changing demand for skills in the labour market (OECD Artificial Intelligence Papers No. 14). OECD Publishing. https://doi.org/10.1787/88684e36-en*
14. *Haq, F. ul, Mohd Suki, N., Zaigham, H., Masood, A., & Rajput, A. (2025). Exploring AI adoption and SME performance in resource-constrained environments: A TOE–RBV perspective with mediation and moderation effects. Journal of Digital Economy. Advance online publication. https://doi.org/10.1016/j.jdec.2025.07.002*
15. *International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system. ISO.*
16. *Kergroach, S. (2025). Emerging divides in the transition to artificial intelligence. OECD Publishing. https://doi.org/10.1787/7a178f29-en*
17. *Le Dinh, T., Vu, M.-C., & Tran, G. T. C. (2025). Artificial intelligence in SMEs: Enhancing business functions through technologies and applications. Information, 16(5), 415. https://doi.org/10.3390/info16050415*
18. *Milanez, A. (2025). Algorithmic management in the workplace: New evidence and policy considerations. OECD Publishing.*
19. *Ng, K. K. H., Chen, C.-H., Lee, C. K. M., Jiao, J., & Yang, Z.-X. (2021). A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives. Advanced Engineering Informatics, 47, 101246. https://doi.org/10.1016/j.aei.2021.101246*
20. *OECD. (2023). OECD Employment Outlook 2023: Artificial intelligence and the labour market. OECD Publishing. https://doi.org/10.1787/08785bba-en*
21. *OECD. (2023a). SME and Entrepreneurship Outlook 2023. OECD Publishing. https://doi.org/10.1787/342b8564-en*
22. *OECD. (2025a). AI adoption by small and medium-sized enterprises: OECD discussion paper for the G7. OECD Publishing. https://doi.org/10.1787/426399c1-en*
23. *OECD. (2025b). Generative AI and the SME workforce: New survey evidence. OECD Publishing. https://doi.org/10.1787/2d08b99d-en*
24. *OECD. (2025c). The adoption of artificial intelligence in firms. OECD Publishing. https://doi.org/10.1787/f9ef33c3-en*
25. *Patrício, L., Varela, L., Silveira, Z., Felgueiras, C., & Pereira, F. (2025). A framework for integrating robotic process automation with artificial intelligence applied to Industry 5.0. Applied Sciences, 15(13), 7402. https://doi.org/10.3390/app15137402*
26. *Rajaram, K., & Tinguely, P. N. (2024). Generative artificial intelligence in small and medium enterprises: Navigating its promises and challenges. Business Horizons, 67(5), 629–648. https://doi.org/10.1016/j.bushor.2024.05.008*
27. *World Economic Forum. (2025a). The Global Risks Report 2025 (20th ed.). https://www.weforum.org/publications/global-risks-report-2025/*
28. *World Economic Forum. (2025b). Global Cybersecurity Outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/*
29. *World Economic Forum. (2025c). The Future of Jobs Report 2025. https://www.weforum.org/publications/the-future-of-jobs-report-2025/*