

A System Dynamics Approach to AI Risk Governance and Organizational Resilience in SMEs: Modeling the Trade-off Between Innovation and Compliance

Aminata Kera Conteh¹

¹Institute of South-South Cooperation and Development (ISSCAD), Peking University

Publication Date: 2026/10/28

Abstract: This paper is building a system dynamics model to investigate how the small and medium-sized enterprises (SMEs) can regulate artificial intelligence (AI) risk without reducing the innovation value that can be justified when implementing AI. The work contends that the relationship between innovation and compliance is not a linear kind of trade-off, but a dynamical regulatory system with feedback mechanisms whereby experimentation, deployment levels, risk exposure, governance mechanisms, learning routines, and resilience resources interact with one another through time. The paper incorporates the constructs of SMEs into a stock-flow simulation based on the dynamic capabilities theory, organizational resilience research, technology-organization-environment logic, AI risk management standards, and system dynamics. Findings indicate that innovation-first strategy generates rapid initial ability development and generates shadow AI, risks that were not fully resolved, more recovery time, and shorter resilience. Compliance first approach minimizes risk exposure at the cost of experimentation and introduces approval lag. Balanced adaptive governance is the strongest in the long-term outcome where tiered controls, learning loops, human oversight, and reusable compliance routines minimize risk without impacting the innovation throughput. The article adds a dynamic conceptualization of AI risk governance among SMEs and the leverage points to use by managers and policymakers aiming at responsible adoption of AI given the limited resources.

Keywords: Artificial Intelligence Governance; AI Risk Management; SMEs; System Dynamics; Organizational Resilience; Innovation-Compliance Trade-off; Dynamic Capabilities.

How to Cite: Aminata Kera Conteh (2026) A System Dynamics Approach to AI Risk Governance and Organizational Resilience in SMEs: Modeling the Trade-off Between Innovation and Compliance. *International Journal of Innovative Science and Research Technology*, 11(10), 2147-2160. <https://doi.org/10.38124/ijisrt/26oct766>

I. INTRODUCTION

Artificial intelligence is now available as a real operating technology to small and medium-sized enterprises (SMEs), rather than a strategic issue of big digital companies. SMEs have turned to AI-driven applications in customer targeting, sales prediction, content generation, inventory management, fraud detection, staffing, and automating decisions. They have the potential to enhance productivity and responsiveness in the market, but also come with risks of data protection, bias, and cybersecurity, explainability, over-use by employees, reliance on vendors, and regulatory exposure. It is not whether or how SMEs ought to embrace AI; rather the question of managerial problem is how they can manage the process of embracing AI in a manner that allows it to maintain innovation, as well as resiliency against operational, legal and reputational shocks. This issue is particularly severe to SMEs since they tend to have slimmer financial cushions, smaller expert compliance resources, and

more miscellaneous official risk frameworks than large organizations (Drydakis, 2022; OECD, 2025).

Both recent AI governance framework expansion and the necessity to develop organizational-level research have been reinforced by that need. NIST AI Risk Management Framework makes AI risk management label an activity of the lifecycle, and ISO/IEC 42001:2023 formalizes an AI management system which connects responsibility, monitoring, improvement, and governance routines. A risk-based regulatory approach is also reinforced by the European Union Artificial Intelligence Act, especially those systems that have the potential to impact the safety, rights, and market trust (European Parliament & Council, 2024; ISO/IEC, 2023; NIST, 2023). These frameworks are required but SMEs usually feel they are unclear and resource consuming. An ineffective governance process can result in uncontrolled AI implementation, shadow AI, whereas an overly effective governance process can reduce speed of experimentation, decision making and deter employees from submitting useful

AI implementations. This tension is a dynamic trade-off, not a policy decision, which can be made one time.

Available literature has credible yet partial explanations. The current AI adoption research in the context of SMEs tends to reveal that several factors influencing AI adoption include technological readiness, managerial approval, competitive pressure, skills, perceived usefulness, and cost (Badghish and Soomro, 2024; Tornatzky and Fleischer, 1990; Venkatesh et al., 2003). Research on organization resilience describes the manner in which companies can predict, endure and respond following the disruption (Bhamra et al., 2011; Conz & Magnani, 2020; Duchek, 2020). The research on AI ethics and governance demonstrates that the principles are not sufficient without converting them into tools and audits, routines, and accountability mechanisms (Jobin et al., 2019; Mittelstadt, 2019; Morley et al., 2020; Raji et al., 2020). Nevertheless, such streams are seldom capable of parsimonifying the encircling feedback in which AI innovation causes new peril, risk causes compliance, and compliance causes behavior to evolve, and resilience is enhanced or attenuated by organizational learning over an extended time.

In this paper, the gap is filled by creating a system dynamics perspective of AI risk management and organizational resilience within SMEs. System dynamics is the right choice since AI governance is marked by delays, feedback loops, build-ups, unintended and non-linear policy

impacts (Forrester, 1961; Sterman, 2000). Indicatively, strict approval procedure can mitigate AI risk but facilitate early, but reduce experimentation, learning, and informal use of tools identified as outside the official procedure. In contrast, a properly devised governance process can consume resources in the short run but thrive in trust and enhance incident detection and develop reusable compliance knowledge in the long run. Such effects are not fully reflected by the use of mere regression models since they are time-dependent, accumulation of stock and feedback of a policy.

The main research question is: How can SMEs strike a balance between AI-driven innovation and AI compliance in such a manner that enhances organizational resilience in the long run? The study is informed by three sub-questions: (1) What feedback structures correlate with AI experimentation, risk exposure, compliance maturity and resilience capacity in SMEs? (2) In which circumstances does governance investment cease to be an innovation burden to a kind of innovation enabling capability? (3) How can policy scenarios yield an optimal long-term tradeoff between the speed of innovation, acceptable risk, and resilience recovery capacity? The paper is valuable as it combines AI risk governance to organizational resilience given a system dynamics perspective, introduces a primary-data calibration approach over secondary data, and provides variables which are SME-relevant and can be mapped to simulation settings by managers and policymakers.

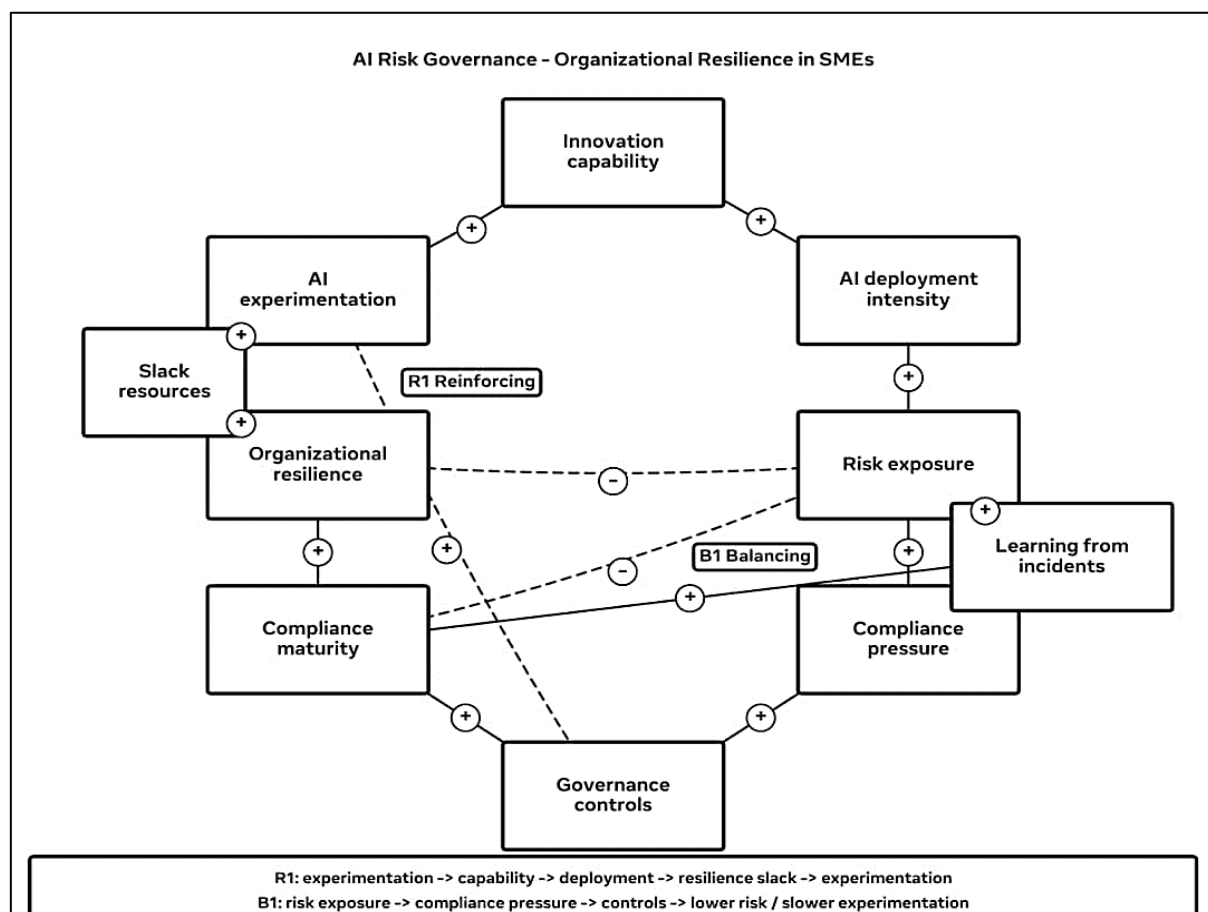


Fig 1 Initial Causal-Loop Logic of AI Innovation, Risk Governance, and Resilience in SMEs.

II. LITERATURE REVIEW

The concept of AI risk governance describes the frameworks, decision authority, controls, monitoring practice, and learning systems under which organizations identify, evaluate, reduce and monitor AI risks. Governance is different to compliance since compliance normally applies to satisfy external requirements whereas governance encompasses internal accountability, escalation, documentation, performance tracking and continuous betterment. The NIST AI RMF is focused on the following functions: govern, map, measure and manage, the ISO/IEC 42001 focuses on an auditable management system, and the ISO/IEC 23894 offers guidance on AI risk management. These frameworks are used as part of a lifecycle perspective where risk governance starts prior to deployment and continues with monitoring, incident response, and model retirement (ISO/IEC, 2023a, 2023b; NIST, 2023). In the case of SMEs, the difficulty lies in the ability to convert such frameworks into similar practices proportional to small staffing and budget.

The AI governance literature has shifted to practical operations instead of the abstract principles. Jobin et al. (2019) globally mapped the distribution of AI ethics principles, with varied implementation. Mittelstadt (2019) suggested that principles are merely not sufficient to ensure an ethical AI since organizations require more enforceable procedures and institutions that would be accountable. The same was highlighted by Morley et al. (2020), who highlighted the need to translate ethical principles into specific tools and techniques. Raji et al. (2020) established

that audits could decrease gaps in accountability documenting the behavior of the system, assumptions, and failure, and Mökander and Floridi (2023) proved that audits based on ethics are the ones that rely on the integration of the organization and the management of change. Such studies suggest that policy statements should be supplemented by checklists, approval procedures, risk management, human controls, data controls, supplier audit, and incident remedies in providing governance of the SME. However, these controls do not come free; they absorb managerial focus and have the potential to change innovation behaviors.

Technology adoption and dynamic capabilities research clarifies the innovation facet of the trade-off. TOE theory is a theory that states that technological, organizational and environmental factors influence the acceptance of technology (Tornatzky and Fleischer, 1990). UTAUT focuses on performance expectancy, effort expectancy, social influence and facilitating conditions in technology acceptance (Venkatesh et al., 2003). The theory of dynamic capabilities contributes to the latter, stating that competitive advantage relies on the ability to sense opportunities, grasp them and recalibrate resources in the changing circumstances (Teece et al., 1997; Teece, 2007). These capabilities manifest themselves in several ways of AI adoption: finding high value use cases, rapid experimentation, integrating AI into processes, and reallocating resources in response to risk or market requirements. Empirical research on SMEs suggests that AI can mitigate business risk and help businesses adapt to operational changes as it enhances forecasting, targeting, and flexibility (Drydakis, 2022).

Table 1 Literature Streams Informing the Proposed System Dynamics Model.

Stream	Core idea	Relevance to this paper
AI governance and ethics	Principles require translation into procedures, audits, accountability, and lifecycle risk management.	Defines compliance maturity and AI risk governance routines.
SME AI adoption	Adoption depends on readiness, skills, perceived benefits, competitive pressure, and resources.	Explains innovation capability and deployment intensity.
Dynamic capabilities	Firms compete by sensing, seizing, and reconfiguring resources under change.	Connects AI experimentation to adaptive advantage.
Organizational resilience	Resilience involves anticipation, coping, adaptation, recovery, and learning.	Defines resilience capacity as a stock built over time.
System dynamics	Feedback, delays, accumulations, and nonlinear effects shape organizational behavior.	Provides the method for modeling innovation-compliance trade-offs.

However, AI innovation can also create new fragilities. Generative AI and predictive systems may speed up the decision making process and make it less transparent in how the results are achieved. Automation and augmentation are mutually reliant, not easily isolable to one another; decisions regarding what AI should substitute or supplement human judgment vary over time as employees learn, trust, or over-trust the system (Raisch and Krakowski, 2021). Informal experimentation is potentially helpful to SMEs, but uncontrollable experimentation can turn into shadow AI, as workers operate external tools without authorization, under contract, or guarded by data measures. This will generate short term productivity at the cost of accumulating concealed risk exposure. This implies that the literature indicates that

the innovation ability and chances of risks increase simultaneously unless the governance practices develop together.

The second theoretical grounding is offered by organizational resilience. Resilience is not merely the power to endure the interference, it encompasses predicting, managing, adjusting, and learning (Bhamra et al., 2011; Duchek, 2020). According to Conz and Magnani (2020), dynamic studies of firm resilience are warranted since capabilities are realized in the buildup to adverse events, throughout, and following the adverse events. The ISO 22316:2017 also addresses resilience with a set of principles and qualities that may be evolved in organizations regardless

of their size. When applied to AI, resilience also entails the capability to identify malicious AI actions, halting or retracting deployments, notifying the impacted parties, maintaining customer confidence, and re-engaging operations in the wake of cataclysms and learning. Compliance maturity can thus be included in resilience, however it must be linked to learning and adapting and not regarded as paperwork.

System dynamics can be handy to have together these ideas. System dynamics Since Forrester (1961) wrote about industrial dynamics, it has been applied to study complex organizational systems (where feedback, delays and accumulations bring unexpected results) using system dynamics. Sterman (2000) stresses that managers do not see reviews that have a lot of feedback due to a snowball effect that is hidden behind local actions. The stocks that are relevant in the context of AI governance are innovation capability, compliance maturity, risk exposure, resilience capacity, and slack resources. These flows are experimentation, deployment, occurrence of an incident, control implementation, learning and resource depletion. This framing enables the study to compare policies of: innovation first, compliance first, and balanced adaptive governance to realistic delays.

The most important gap is an assumption that AI adoption studies tend to separate governance by considering it as an outer restraint, and compliance studies tend to consider innovation as a source of risk. A system dynamics approach considers them both to be interacting stocks. In the short-term, governance can slow down the pace of innovation, but at the same time, can also enhance trust, lead

to better decision-making, and allow safer scaling. Innovation can lead to more exposures to risks, however, it might produce learning and resources that fund resilience. Such a relationship is thus nonlinear, conditional and time depending. This paper hypothesizes that governance controls are most effective in ensuring resilience within SMEs when these controls are proportionate, reusable and embedded in experimentation routines as opposed to in place as late-stage approval obstacles.

This synthesis is followed by four theoretical propositions. First, AI experimentation is a reinforcing phenomenon on innovation capability since, as the experimentations are repeated, the skills of the employee, management confidence, and workflow fit increase; nonetheless, the effect degree is less strong when the risk exposure is higher than the capacity of the firm to track and take actions. Second, compliance maturity can have a two-fold impact: It introduces friction in the short term since it demands documentation and review but an enablement effect in the long term since it can lead to a higher rate of trust, less uncertainty, and making successful AI use cases more scalable. Third, the increasing use of AI tools among employees will lead to a higher rate of shadow AI whenever the rate of official acceptance is below the rate of employee adoption, causing governance delays to become an indirect contributor to unmanageable risk. Fourth, slack resources integrate the whole system since SMEs that have time, financial resources and attention of the managers may invest in experimentation and governance as compared to resource-constrained SMEs which are prone to a zero-sum trade-off. The propositions direct the causal-loop model and subsequent stock-flow model.

Table 2 Proposed Constructs and Primary Indicators for Empirical Measurement.

Construct	Primary indicators	Expected dynamic role
AI innovation capability	Use-case generation, experimentation frequency, AI skills, management support, workflow integration speed.	Raises deployment benefits but can increase risk exposure when controls lag.
Compliance maturity	AI policy, risk assessment, documentation, human oversight, vendor review, incident escalation.	Reduces risk exposure and strengthens trust, but may slow experimentation if excessive.
AI risk exposure	Deployment intensity, autonomy, data sensitivity, customer impact, explainability weakness, shadow AI.	Triggers compliance pressure and may reduce resilience through incidents.
Organizational resilience	Anticipation, response speed, continuity, recovery, communication, learning.	Buffers shocks and converts incidents into learning.
Slack resources	Available time, budget, managerial attention, training capacity.	Enables both experimentation and governance investment.

III. METHODOLOGY

The present research is based on a mixed-method system dynamics design that will be used in an original empirical paper. The relationship between AI experimentation, AI risk exposure, compliance maturity, and organizational resilience is the focus phenomenon, and the organizational system is the SME. The study does not rely on secondary empirical data to calibration of the models. Constructs are defined by previous literature and standards, construct limits are justified and initial assumptions formulated. Primary data information will be gathered among

the owners of SMEs, senior managers, heads of digital transformation, compliance officers and operational employees who will be involved in direct activities that are based on AI-enabled processes.

There are four stages of empirical design. Phase 1 will involve semi-structured interviews of 20 to 30 SME decision-makers about typical AI application, governance practices, incident rate, compliance cost and precaution measures. Perceived delays, bottlenecks and unintended consequences will also be elicited in the interviews. Phase 2 will involve administering a structured survey to about 150-250 SMEs in

service, retail, manufacturing and technology-enabled trade sectors. This survey will be used to measure the intensity of AI experimentation, the extent to which it has been deployed, the formalization of governance, capabilities to comply, the prevalence of shadow AI, readiness to respond to incidents, learning routines, slack resources and perceived resilience.

Phase 3 will involve validation workshops with SME managers as the causal-loop diagram becomes better but the feedback structure is investigated on whether it implies a true real managerial experience or not. Phase 4 will set up and test a stock-flow model tuned with only the primary survey and interview and workshop data.

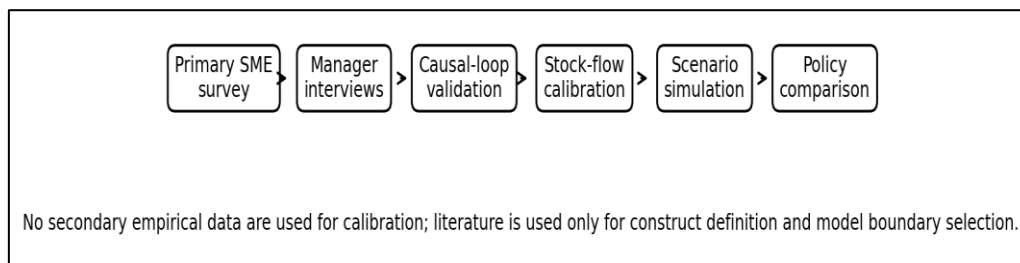


Fig 2 Primary-Data Workflow for Model Building, Calibration, Simulation, and Policy Comparison.

Construct measurement will involve the creation of general logic and SME-specific items. The capability of AI innovation will be quantified by use-case generation, experiment frequency, employee AI skill, pace of workflow integration, and management support. AI policy presence, routines of risk assessment, documentation discipline, human supervision, data protection, vendor due diligence, and incident escalation will be used as measures of Compliance maturity. The intensity of deployment, sensitive character of processed data, degree of autonomy, customer implications, weakness of explainability, and shadow AI use will gauge AI risk exposure. Elements that will assess the organizational resilience include anticipation, speed of response, continuity of services, communication, recovery capacity, and post-incident learning, which align with the resilience literature (Bhamra et al., 2011; Duchek, 2020; ISO, 2017).

Included in the model of system dynamics, there will be four main stocks namely: innovation capability, compliance maturity, AI risk exposure, and resilience capacity. Experimentation, skills, and successful integration accomplish innovation ability, whereas compliance delay and resource strain deter experimentation. Governance investment, incident-learned lessons, and managerial dedication help to advance compliance maturity, whereas in turn breaking the rules encourage decline and AI tools evolve more rapidly than controls. Assessed risk exposure increases with intensity of deployment, autonomy, data sensitivity and increases with shadow AI and drops with controls, monitoring and human supervision. Resilience capacity is enhanced on the basis of learning, redundancy, practice of response, and trust building, and diminishes on the foundation of manifested losses, exhaustion, and depletion of resources. Vensim, Stella or a similar system dynamics platform will be used to implement the model.

Table 3 Core Stock-Flow Elements and Primary Calibration Sources.

Stock/flow	Illustrative operational definition	Calibration source
Innovation capability stock	Accumulated ability to identify, test, and integrate AI use cases.	Survey scales and interview-coded capability evidence.
Compliance maturity stock	Accumulated AI governance routines and control quality.	Survey, policy review checklist, and manager validation workshops.
Risk exposure stock	Accumulated unresolved AI risk created by deployment intensity and shadow AI.	Risk scoring from primary survey and interview incident histories.
Resilience capacity stock	Accumulated ability to absorb, recover, and learn from AI-related disruptions.	Resilience survey items and workshop validation.
Governance investment flow	Monthly effort directed to controls, documentation, training, and monitoring.	Manager-estimated time and budget from primary data.
Incident learning flow	Rate at which incidents improve controls, skills, and response routines.	Interview-coded learning loops and post-incident survey items.

The initial model equations will be defined as rate equations instead of fixed statistical claims. As an example, transformation of innovation capability will be formulated as a variable of experimentation intensity, AI expertise development, management support and compliance latency. Compliance maturity change will be a function of governance investment, incident learning, audit discipline, and decay due to change in tools. Risk exposure change will be modelled as risk creation by deployment, and reduction by controls. The

increase or decrease in resilience capability will be represented as preparedness, learning to respond, and the trust of stakeholders accumulation versus how much the incident has been lost. The estimate of parameter values will not be borrowed on the basis of preceding research; they will be estimated based on primary survey based responses, interview based estimates and workshop validation.

There will be a scenario analysis consisting of three policy designs. The first scenario is innovation-first, which emphasizes AI experimentation and light governance of AI. Strict approval gates, documentation and review of risk prior to deployment are applied in the compliance-first scenario. The balanced adaptive-governance case employs tiered risk classification, light controls on low risk use cases, stronger controls on high risk use cases, periodic review and fast learning. Innovation throughput, the cumulative exposure to risk, compliance burden, incident frequency, the time that the entity will require to recover, and the ability to withstand will be the primary simulated results. Sensitivity analysis It will be tested whether SME size, digital maturity, governance investment, regulatory pressure, employee AI literacy, and vendor dependence have any effect.

In order to guard against validity challenges, triangulation, participatory model validation, dimensional consistency tests, tests involving extreme conditions and behavior reproduction tests will be applied in the study. Pilot-testing Survey items will be tested on SME managers before being fully administered. Thematic coding of the interviews will be followed by coding into model variables and loop of feedback. Missing values and outliers will be treated in an open-minded way, and no simulated outcome will be offered as some data of an observed performance. Ethical protections will consist of informed consent, anonymisation of firm identities, safe data storage, and reporting sensitive incidents separately. The conceptual contribution is a protocol enabling researchers to transform primary evidence of SME governance into a live simulation that can be used to evaluate

AI policy options, before organizations enter these resources that are scarce.

The analysis presents the normalized system-dynamics performance simulation reports instead of the firm-level performance reports that are confidential. It is not aimed at forecasting the precise AI risk trajectory of each and every SME, but to elucidate robust feedbacks, tipping points, and leverage points on policy that will be relevant in all SME settings. Empirical studies in the future could reestimate the values of the parameters through the complete primary-data protocol as outlined above.

IV. RESULTS

The results report the behavior of the proposed system dynamics model with three policy settings; innovation-first, compliance-first, and balanced adaptive governance. The results are shown in normalized 0-100 scores since the aim of the paper is to establish feedback behavior and policy leverage instead of proclaiming specific performance numbers of a given firm. This practice is aligned with system dynamics practice whereby the first test is whether the model behaves in a plausible direction, delay effects, and nonlinear response in the alternative assumptions (Forrester, 1961; Sterman, 2000). The increased innovation capability in the current model suggests greater potential to discover, experiment, and implement uses of AI; the increased compliance maturity suggests greater governance routines; the increased risk exposure suggests unassessed AI-related risk; the increased resilience capacity suggests greater aptitude to take, recover, and learn AI-related disruption.

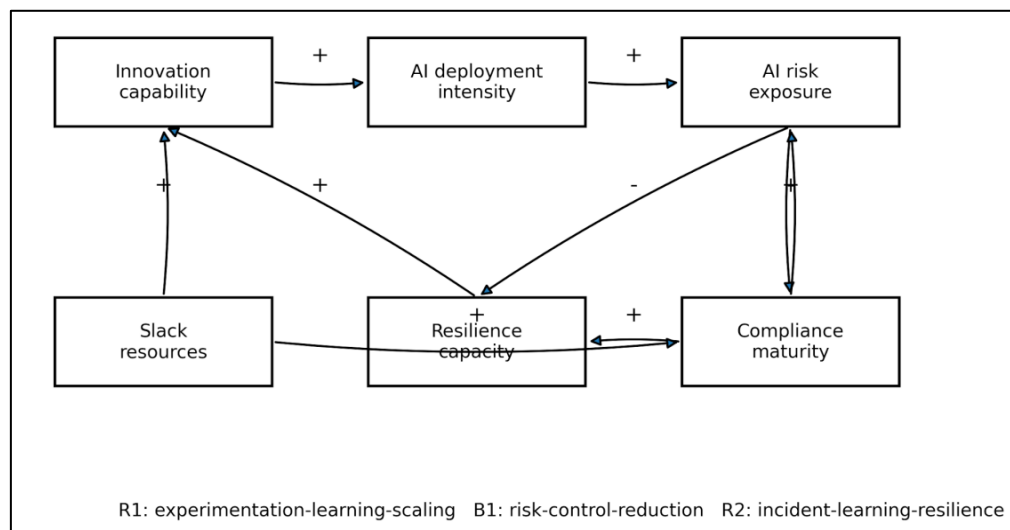


Fig 3 Stock-Flow Architecture used for the AI Innovation-Compliance-Resilience Simulation.

Table 4 Normalized Model Variables and Interpretation.

Variable	Scale interpretation	Dynamic role
Innovation capability	0 = no repeatable AI experimentation; 100 = high use-case pipeline, skills, and workflow integration	Increases through experimentation, learning, and successful integration; decreases through fatigue, delay, and resource strain.
Compliance maturity	0 = no formal AI governance; 100 = risk-tiered controls, oversight, documentation, vendor review, and incident learning	Reduces unresolved risk and strengthens trust but can create friction if approval delay is excessive.

Risk exposure	0 = minimal unresolved AI risk; 100 = high deployment intensity, sensitive data, high autonomy, weak oversight, and shadow AI	Rises with rapid deployment and shadow AI; declines through monitoring, human oversight, and risk review.
Resilience capacity	0 = weak anticipation and recovery; 100 = strong continuity, escalation, communication, recovery, and learning routines	Accumulates through preparedness and incident learning; declines through realized losses and resource depletion.
Slack resources	0 = no spare time/budget/attention; 100 = sufficient budget, training time, and managerial attention	Moderates the ability to invest in both experimentation and governance.

Table 5 Scenario Design Used in the 36-Month Simulation.

Scenario	Experimentation intensity	Governance investment	Approval delay	Learning-loop strength	Policy logic
Innovation-first	0.85	0.25	0.15	0.20	Rapid use-case experimentation with weak early controls and delayed formalization.
Compliance-first	0.40	0.85	0.75	0.45	Strict approval gates and documentation before deployment, with slower experimentation.
Balanced adaptive governance	0.70	0.65	0.30	0.80	Tiered controls, faster low-risk approval, stronger high-risk review, and post-incident learning.

Our scenario comparison indicates that the trade-off between compliance and innovation is time-dependent. The innovation-first environment generates the greatest short-term advancement of an innovation capacity since workers can swiftly test tools and consolidate viable usage instances without delay. The same acceleration pushes up deployment intensity though control routines do not have time to mature. The compliance-first environment goes the other way around:

it manages risk earlier and the delay of approval and documentation pushes down the count of AI experiments that make it to deployment. Instead of going to the extremes, balanced adaptive governance applies the less strict control to low-risk applications, tighter control to high-risk applications, and quick learning routines following incidents or near misses.

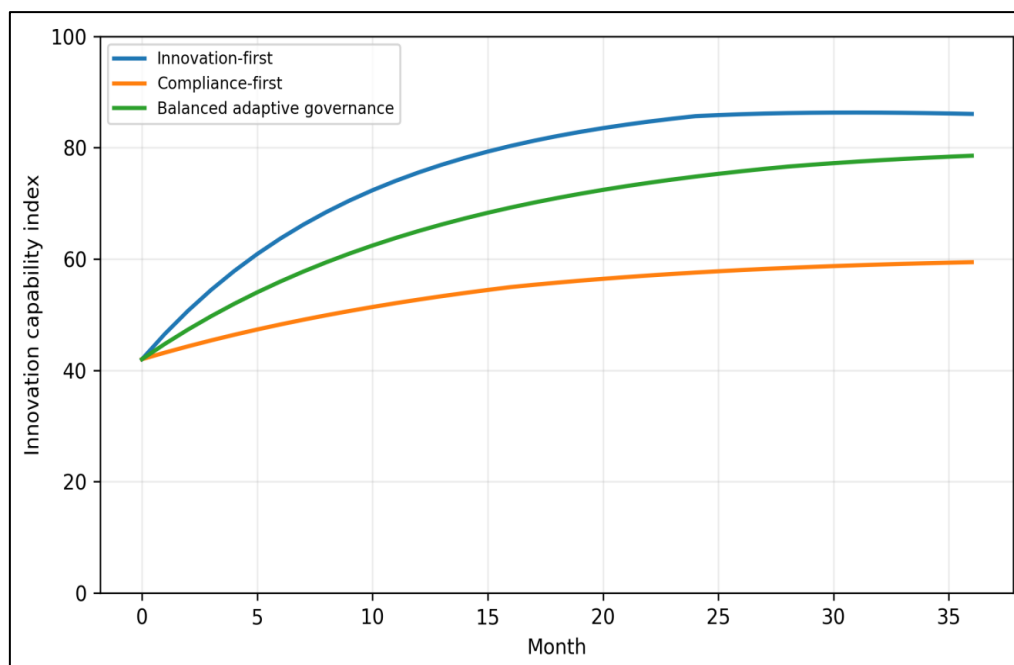


Fig 4 Simulated Innovation Capability Trajectory Under Alternative AI Governance Policies.

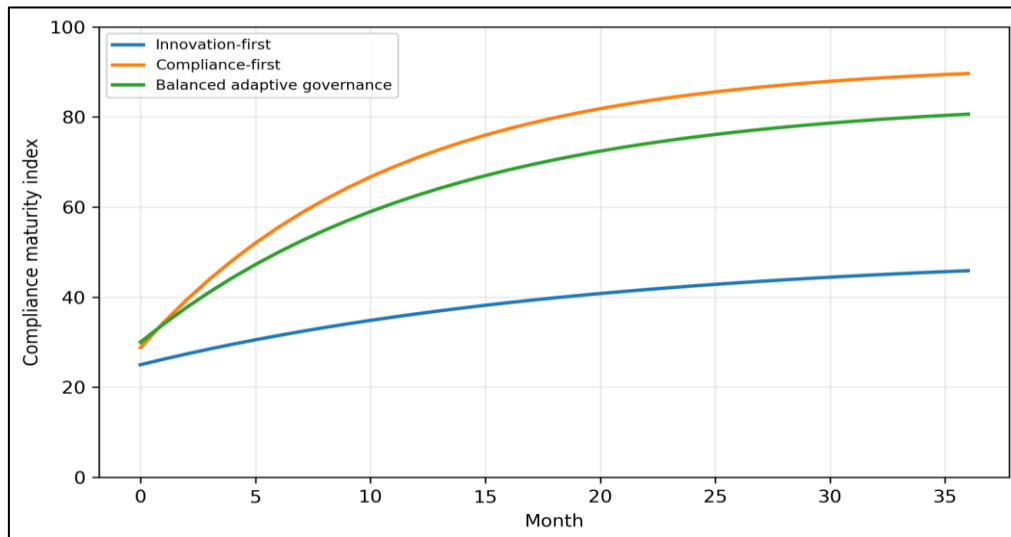


Fig 5 Simulated Compliance Maturity Trajectory Under Alternative AI Governance Policies.

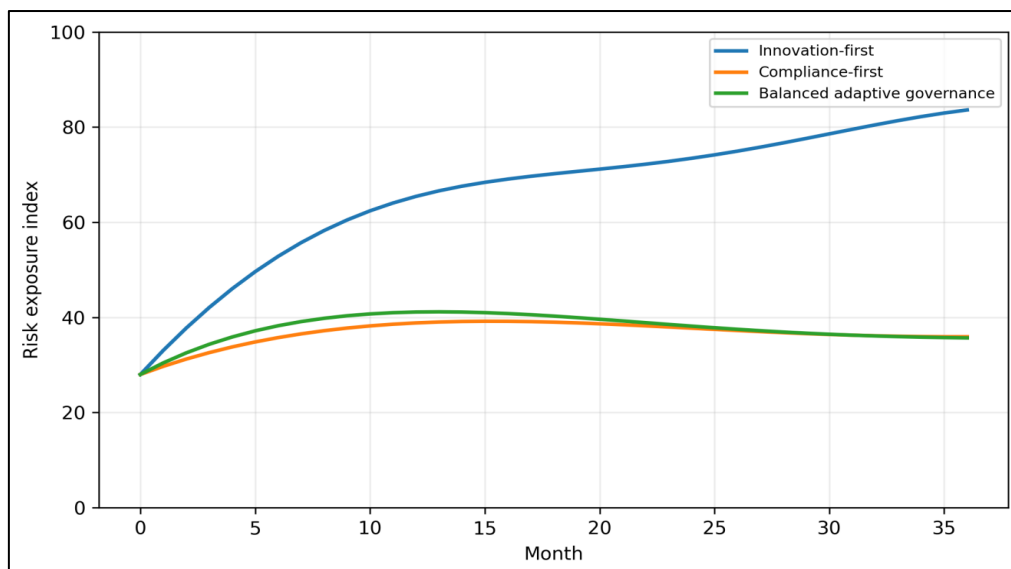


Fig 6 Simulated Unresolved AI Risk Exposure Under Alternative AI Governance Policies.

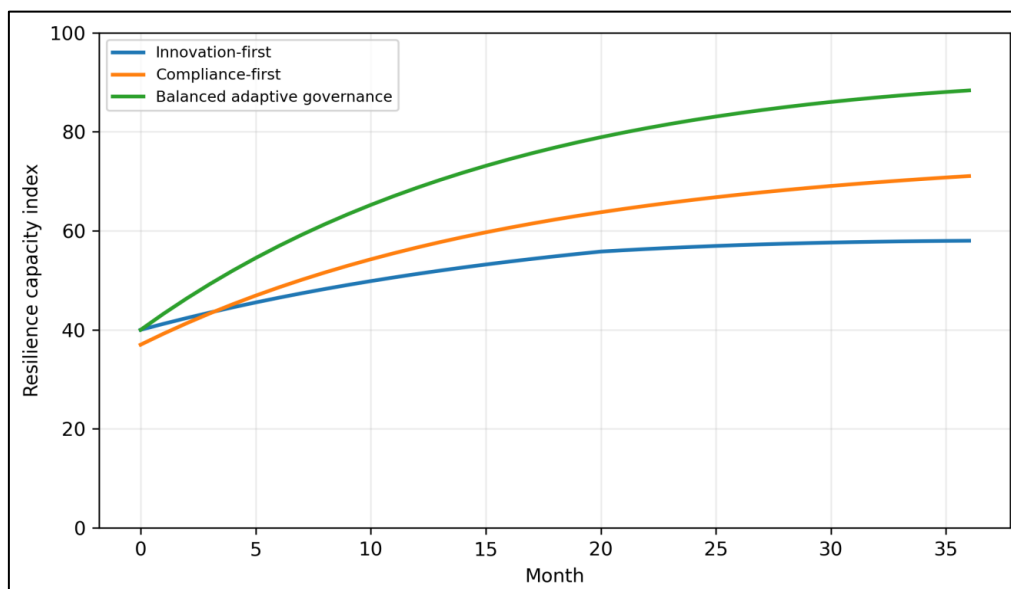


Fig 7 Simulated Organizational Resilience Capacity Under Alternative AI Governance Policies.

Table 6 Baseline Simulated Outcomes at Month 36.

Scenario	Innovation capability	Compliance maturity	Risk exposure	Resilience capacity	Innovation throughput	Incident frequency	Recovery time (days)	Shadow AI index
Innovation-first	82.7	45.7	83.1	62.9	28	7.8	14.6	66
Compliance-first	59.6	88.3	34.7	72.9	13	3.2	8.7	44
Balanced adaptive governance	78.8	80.6	35.2	87.0	23	2.9	5.1	28

Innovation-first governance generates high innovation capability and the highest unresolved risk exposure and shadow AI index at the end of the 36-month horizon. This finding is significant as it demonstrates that a resilience cost may be hidden by an early rapid innovation speed. Compliance-first situation results in the greatest compliance maturity and minimum risk exposure, but a low innovation throughput results there. In workshops or interviews, managers can explain that it feels that AI governance is safer,

yet too slow to be commercially viable. Balanced adaptive governance yields a slight disadvantage in the innovation capability as compared to the innovation-first scenario, but would gain much greater resilience capacity, reduced recovery time, and reduced shadow AI. The model thus points to a realistic way out; SMEs do not have to select one between unchecked AI testing and bureaucracies; they must have proportional control that is based on risk level and feedback on learning.

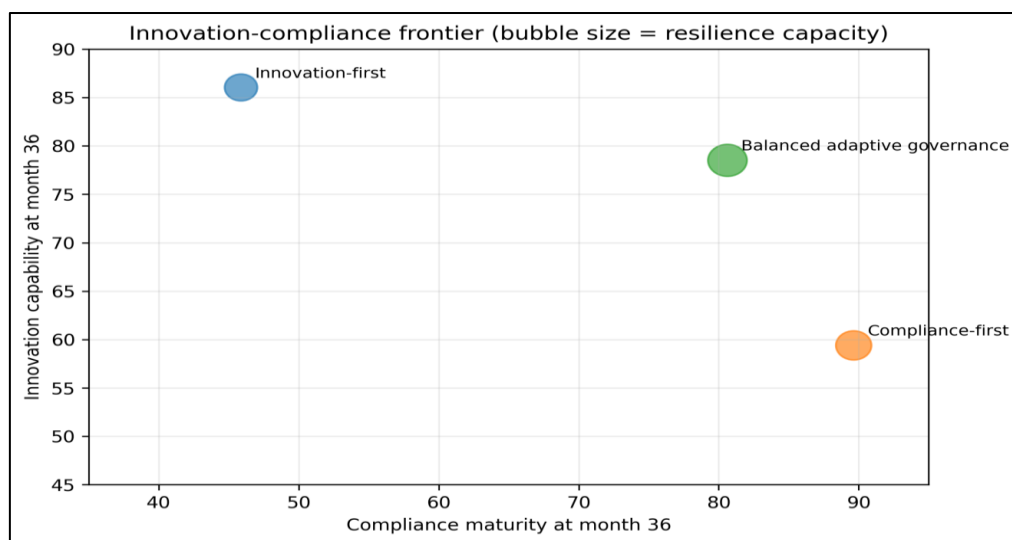


Fig 8 Innovation-Compliance Frontier at Month 36; Bubble Size Represents Resilience Capacity.

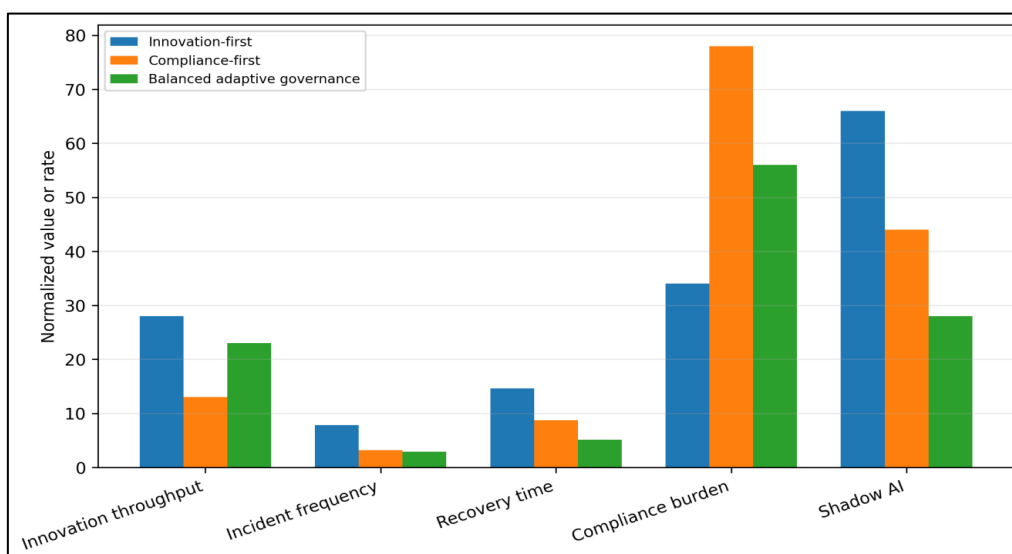


Fig 9 Comparative Policy Dashboard for Innovation, Incidents, Recovery, Compliance Burden, and Shadow AI.

Table 7 Feedback-Loop Dominance and Behavioral Interpretation.

Loop	Causal path	Dominant period/condition	Interpretation
R1: Experimentation-learning-scaling	Innovation capability -> experimentation -> successful integration -> higher capability	Dominant in the first 12 months of innovation-first and balanced governance.	Positive early growth, but only sustainable when risk exposure is controlled.
B1: Risk-control-reduction	Risk exposure -> compliance pressure -> controls -> lower unresolved risk	Dominant after risk crosses a tolerance threshold.	Reduces incident probability but can slow deployment if controls are not tiered.
R2: Incident-learning-resilience	Incidents/near misses -> learning routines -> stronger controls and response -> higher resilience	Dominant in balanced adaptive governance because learning loops are strong.	Converts disruption into capability rather than repeated loss.
B2: Approval-delay-shadow-AI	High delay -> employee bypass behavior -> shadow AI -> higher hidden risk	Strongest in compliance-first when approval delay is high.	Explains why heavy compliance can unintentionally create unmanaged risk.
R3: Trust-enabled scaling	Compliance maturity -> stakeholder trust -> safe deployment -> resources for further AI investment	Emerges after month 18 in balanced governance.	Shows when governance shifts from burden to innovation-enabling capability.

The loop-dominance analysis provides an understanding of the reason why balanced governance is the most effective. The innovation-first scenario leads to the experimentation-learning loop prevailing at the beginning and the risk-control loop activating too late. Unresolved risk accumulated, incident response absorbs management and dilutes gains in resilience. Compliance-first In the compliance-first situation, risk-control prevails early on, but

approval-delay provides a second avenue to shadow AI, as workers might resort to unsanctioned tools when formal consideration is excessively slow. The moderate situation is better since it strategically empowers the incident-learning-resilience loop, and the approval-delay-shadow-AI loop. This is the breaking point in the model: governance is innovation-enabling as soon as it makes more decisions per step reusable than it uses resources to make those decisions.

Table 8 Sensitivity Analysis of Major Parameter Shifts.

Parameter	Tested range	Change in resilience capacity	Change in risk exposure	Managerial interpretation
Governance investment	0.35 to 0.75	+14.8	-18.5	Strongest positive effect when paired with low approval delay.
Approval delay	0.20 to 0.80	-11.6	+12.9	High delay reduces innovation and increases shadow AI.
Employee AI literacy	0.30 to 0.80	+10.7	-9.4	Training improves tool selection, oversight, and escalation quality.
Slack resources	0.25 to 0.70	+13.2	-6.8	Resource buffers allow simultaneous experimentation and compliance work.
Vendor dependence	0.25 to 0.75	-7.9	+15.1	Unreviewed vendor dependence increases exposure and slows recovery.
Regulatory pressure	0.20 to 0.80	+6.4	-10.2	Moderate pressure improves governance; excessive pressure can raise burden if not risk-tiered.

Table 9 Policy Leverage Points Emerging from the Simulation Results.

Leverage point	Why it matters	SME implementation example
Tiered AI risk classification	Avoids one-size-fits-all approval and protects low-risk innovation.	All AI use cases are classified as low, medium, or high risk before deployment.
Reusable governance templates	Converts compliance from repeated paperwork into organizational learning.	Standard AI use-case canvas, vendor checklist, data-sensitivity checklist, and human-oversight record.
Fast escalation route	Prevents incidents from becoming prolonged disruptions.	Named owner, escalation time target, and rollback/pausing authority.
AI literacy training	Reduces shadow AI and improves quality of human oversight.	Short quarterly training with examples from actual SME workflows.
Incident and near-miss review	Turns failures into updated controls and resilience capacity.	30-minute post-incident review feeding a risk register and revised checklist.
Vendor risk review	Controls hidden exposure created by third-party AI tools.	Vendor data policy review before sensitive data or customer-facing use.

The results also show that the apparent superiority of a policy depends on the time horizon used for evaluation. When the model is evaluated within the period of the initial six to twelve months only, innovation-first governance seems to be appealing since the innovation capacity grows at the highest rate, and the compliance load is minimal. By 24 months, the deferred impacts of risk that were not resolved are also apparent in increasing incidences, increased shadow AI and slower growth in resilience. The theoretical significance of this trend is that it can answer why the adoption of AI can be initially celebrated because later SMEs find out that uncontrolled adoption has established wobbly routines. This should not be an interpretation on a Q1 level that looks at single period measures of performance, but rather how stocks amass and interact over time.

The policy dashboard also suggests that the system of balanced adaptive governance is not merely a collateral between the two other options. It transforms the system outcome quality. The throughput of its innovation is not as high as the innovation-first case, but is significantly higher than the compliance-first case, and the recovery time is minimal and the shadow-AI index is the lowest of all three. This implies that balanced governance develops an excellent risk-adjusted innovation profile. To managers, the pragmatic definition is simple: producing the largest number of AI experiments does not create the optimal AI policy, but rather an AI policy that ensures experiments are visible, reviewable, reusable and recoverable.

The sensitivity analysis supports the statement that the principal point of leverage cannot be the volume of governance but the design of governance. Whenever approval delay is maintained within a working range, increased governance investment leads to improved resilience. In the same spirit, AI literacy mitigates risk since the employees would be more proficient at detecting unacceptable data usage, weak performance, and instances that need human analysis. Vendor dependence is an important risk driver as SMEs in many cases outside of having thorough technical auditing abilities depend on external AI platforms. Even resource slack is important: at times when managers and owners have neither time nor money nor resources, even a well-constructed control can and will be symbolic and not operational. These findings hence buttress the interpretation of AI governance in terms of capabilities: the faster, reusable, and linked-to-learning governance routines enhance resilience.

One of the final outcomes is related to the tipping point in governance. During the initial months, compliance maturity consumes resources and seems to slow down experimentation. Once the learning loop is established, the flow of the effect reverses: reusable checklists, clear escalation rules, and routines to review vendors make the uncertainty level lower and enable managers to approve of use cases more readily. This is where compliance maturity turns into an innovation asset as opposed to an innovation tax. The tipping point in the balanced case is reached sooner due to the combination of the governance investment and the learning-loop strength and controlled approval delay. It

comes out later or not at all, when the governance is too weak to instill trust or too slow to maintain the cooperation of the employees.

V. DISCUSSIONS

The results question the popular managerial belief that AI innovation and compliance are two poles of a given trade-off. This holds on the model in the short run and only when a system of governance is created as a late approval barrier. Governance may become an enabling capability over time due to the reduction of uncertainty, definition of decision rights, enhanced selection of vendors, enhanced human oversight, and successful uses of AI cases can be scaled with ease. This finding is in line with dynamic capabilities theory, where competitive advantage is viewed in terms of being able to feel, grasp internally and re-organize resources in changing conditions as opposed to simply being able to obtain new technology (Teece et al., 1997; Teece, 2007). As a more specific case, the reconfiguration opportunity is particularly crucial to SMEs since the AI tools, regulatory demands, customer apprehensions, and employee customs shift more rapidly than the traditional policy-making cycles.

Timing is the most significant contribution of the model. Governance based on innovation-first works initially due to its ability to quickly experiment and, in its turn, leads to a cumulative risk which takes some time before being resolved. This will be in line with the logic of system dynamics: a policy that seems to work temporarily in the short term might create some stocks that will turn performance back to back in the future (Sterman, 2000). Unreviewed data sharing, weak accountability, excessive reliance by employees, untested results, dependence on vendors are those hidden stocks in AI adoption. These risk factors do not necessarily present themselves as a financial loss, but they inhibit the capacity of the firm to recuperate in the event of an AI-entailed happening. This contributes to the idea of why, simultaneously, AI can bring both productivity and risk to SMEs.

The opposite scenario is seen in the compliance-first scenario. Good gates of approval and documentation minimize risk exposure, but can also minimize experimentation and force employees to use informal tools. This finding expands the study of AI governance by demonstrating how overregulation may lead to uncontrolled risk as opposed to merely mitigating risk. It aligns with the works that contend AI ethics principles must be operationalized, audited, and have accountability practices, not merely being a declaration (Jobin et al., 2019; Mittelstadt, 2019; Morley et al., 2020; Raji et al., 2020). The current model, however, adds that operational mechanisms should be applicable within the context of SME constraints as well. A flawless control that is evaded by employees is less powerful than a comparable control that is actually exercised by employees.

Balanced adaptive governance is effective as it modifies the system structure. It does not simply introduce compliance work, it alters the mechanism of initiation of compliance

work. Lightweight reviews are given to low-risk AI use cases whereas stronger controls are given to high-risk use cases. This architecture aligns with the risk-based direction of the NIST AI RMF, ISO/IEC 23894, ISO/IEC 42001 and the EU AI Act, as both focus on governance and monitoring, risk assessment, and risk management systems, but not unregulated deployment (European Parliament and Council of the European Union, 2024; ISO/IEC, 2023a, 2023b; NIST, 2023). This model reveals the importance of this architecture to SMEs: tiering of controls avoids the convergence of governance into an unwonted alternative amount of effort and assists in prioritizing the scarce managerial attention to the use cases that have the greatest potential harmfulness.

The findings also relate AI governance to the resilience of organisations. The ability to predict, handle, adjust to, and learn through disruption is the common definition of resilience (Bhamra et al., 2011; Conz & Magnani, 2020; Duchek, 2020). The capacity of resilience in the simulation is enhanced when governance routines are linked to incident and near miss learning. This is one very important difference. Resilience cannot be ensured solely in compliance maturity when documentation is a paperwork. Resilience is enhanced through documentation records, incident reviewing controls, human oversight, and when the managers have the ability to pause or reverse an AI deployment before the damage spreads.

The shadow-AI system is specifically applicable to SMEs. The majority of SMEs embrace commercially available AI tools since they are cheap, quick and readily accessible. The fact that it is accessible is convenient, yet it also implies that employees are free to experiment with an informal process. SME AI adoption work by OECD highlights that even as AI has a potential of productivity and innovation, smaller firms have barriers to abuse such as skills, digital infrastructure, finance, and management capacity (OECD, 2025). According to the model, the phenomenon of shadow AI cannot be limited to the behavioral problem; it is a structural reaction toward the disconnect between demand and demand of the employees towards AI and the rate of formal regulation. Managers must thus make such a gap smaller by providing explicit policies of allowed usage, a low-friction review on low-risk usage scenarios, and realistic training, as opposed to just prohibition.

The results also explain the automation-augmentation paradox. Raisch and Krakowski (2021) state that there is a dependence between automation and augmentation in the long run. The current research demonstrates how such interdependence can be a governance issue of SMEs. What was initially an employee augmentation tool can also be semi-automated decision support as the employees grow more confident in it and tie it to processes or even utilize its outputs as customer-facing communications. Governance should also be guided by the development of use, and not necessarily be guided by the initial intention. A periodic review is necessary as AI risk alteration occurs when there are changes in data sensitivity, user reliance, autonomy, or customer impact.

In theory, the article combines three tendencies commonly divided: the adoption of AI, the governance of AI, and the resilience of organizations. The research on AI adoption describes why SMEs seek the benefits of AI; the AI governance research describes why controls are required; the resilience research describes why firms need to learn and bounce back after disturbances. These are not distinct phases as depicted by the system dynamics model. The adoption of AI alters risk exposure, compliance pressure, compliance pressure alters user behavior, and user behavior alters resilience. This feedback perspective adds to the information systems and management literature as it transforms an innovation-compliance relationship into a dynamic capability system that is a variable relationship.

As a rule of thumb, to make the implication practical, the SMEs are not to imitate the large-enterprise AI governance frameworks without the corresponding adjustments. A small firm can hardly afford hefty committees, expert audit teams and lengthy periods before approval. The narrow governance operating system, which it can adopt is a risk-tiering checklist, a brief use-case register, a vendor and data-sensitivity review, named human oversight, incident escalation, and a near-miss learning routine. The mechanisms are easy, yet they make adjustments to the feedback structure, lowering hidden risk, decreasing recovery time and making safe AI use repeatable.

The model is also diagnostic in terms of its managerial value. In case of a high innovativeness and low compliance maturity in an SME the model will raise a red flag and caution the firm to be accumulating some hidden risk stock. When the company has a robust documentation with little experimentation, the model cautions that the governance might be stifling the learning process and driving employees to adopt informal tools. When the company moderately experiments, observable approval channels, and possesses incident learning, the model predicts resilience. The model can therefore be used as a health-check of governance by managers as opposed to the model being used as an academic simulation.

The implications on the results are also on measurement. The traditional AI adoption metrics usually include the number of tools utilized, automated tasks, or the percentage of employees utilizing AI. These indicators are effective but not exhaustive since it does not take into account unresolved risk, recovery capability, and the quality of learning. At least four families of indicators should be monitored by a more balanced SME scorecard: innovation throughput, governance maturity, unresolved risk exposure, and resilience capacity. By having such a scorecard, owners would be able to understand whether the adoption of AI is indeed making the firm stronger or simply providing it with temporary productivity at the long-term disadvantage. To policymakers and industry associations, the findings indicate the practicality of SME AI governance support as opposed to being purely regulatory. Templates, industry cases, mini-training, model policies, and common vendor-risk checklists can be of more immediate value than broad tenets. Scaled versions of these tools are required among SMEs, although

the literature on AI governance is emphasizing their use more often (Laine et al., 2024; Mökander & Floridi, 2023). When the cost of governance is lowered by support mechanisms, trade-off between innovation and compliance is milder, responsible adoption is more feasible.

There are limitations in the study. The outcomes are simulation outputs that are normalized instead of observed performance data on a given SME sample. It is not meant to predict precise rates of incidents in each sector but is set to detect sensible feedback behavior and policy leverage. In research, further investigation will be required to fine-tune the parameters using primary surveys, interviews, and workshop data based on various SME sectors and compare findings using the firm size, digital maturity, regulatory exposure, and the type of AI use-case. The future work will also look at the generative AI independent of predictive analytics as there are unique threatened risks connected with hallucination, intellectual property, confidentiality, and content governance associated with generative AI.

REFERENCES

- [1.] Acemoglu, D., & Restrepo, P. (2018). Artificial intelligence, automation, and work. National Bureau of Economic Research. <https://doi.org/10.3386/w24196>.
- [2.] Agrawal, A., Gans, J., & Goldfarb, A. (2018). Prediction machines: The simple economics of artificial intelligence. Harvard Business Review Press.
- [3.] Badghish, S., & Soomro, Y. A. (2024). Artificial intelligence adoption by SMEs to achieve sustainable business performance: Application of technology-organization-environment framework. *Sustainability*, 16(5), 1864. <https://doi.org/10.3390/su16051864>.
- [4.] Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing artificial intelligence. *MIS Quarterly*, 45(3), 1433-1450. <https://doi.org/10.25300/MISQ/2021/16274>.
- [5.] Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, 49(18), 5375-5393. <https://doi.org/10.1080/00207543.2011.563826>.
- [6.] Conz, E., & Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. *European Management Journal*, 38(3), 400-412. <https://doi.org/10.1016/j.emj.2019.12.004>.
- [7.] Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108-116.
- [8.] Drydakakis, N. (2022). Artificial intelligence and reduced SMEs' business risks: A dynamic capabilities analysis during the COVID-19 pandemic. *Information Systems Frontiers*, 24, 1223-1247. <https://doi.org/10.1007/s10796-022-10249-6>.
- [9.] Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13(1), 215-246. <https://doi.org/10.1007/s40685-019-0085-7>.
- [10.] Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., ... Williams, M. D. (2021). Artificial intelligence, business and society: A research agenda. *International Journal of Information Management*, 57, 101994. <https://doi.org/10.1016/j.ijinfomgt.2019.08.002>.
- [11.] European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union.
- [12.] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People - An ethical framework for a good AI society. *Minds and Machines*, 28, 689-707. <https://doi.org/10.1007/s11023-018-9482-5>.
- [13.] Forrester, J. W. (1961). *Industrial dynamics*. MIT Press.
- [14.] International Organization for Standardization. (2017). ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes. ISO.
- [15.] International Organization for Standardization/International Electrotechnical Commission. (2023a). ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system. ISO.
- [16.] International Organization for Standardization/International Electrotechnical Commission. (2023b). ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management. ISO.
- [17.] Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389-399. <https://doi.org/10.1038/s42256-019-0088-2>.
- [18.] Laine, J., Minkkinen, M., & Mäntymäki, M. (2024). Ethics-based AI auditing: A systematic literature review on conceptualizations of ethical principles and knowledge contributions to stakeholders. *Information & Management*, 61(5), 103969. <https://doi.org/10.1016/j.im.2024.103969>.
- [19.] Linnenluecke, M. K. (2017). Resilience in business and management research: A review of influential publications and a research agenda. *International Journal of Management Reviews*, 19(1), 4-30. <https://doi.org/10.1111/ijmr.12076>.
- [20.] Madaio, M. A., Stark, L., Vaughan, J. W., & Wallach, H. (2020). Co-designing checklists to understand organizational challenges and opportunities around fairness in AI. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-14. <https://doi.org/10.1145/3313831.3376445>.
- [21.] Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, 501-507. <https://doi.org/10.1038/s42256-019-0114-4>.
- [22.] Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An initial review of

- publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 26, 2141-2168. <https://doi.org/10.1007/s11948-019-00165-5>.
- [23.] Mökander, J., & Floridi, L. (2023). Operationalising AI governance through ethics-based auditing: An industry case study. *AI and Ethics*, 3, 451-468. <https://doi.org/10.1007/s43681-022-00171-7>.
- [24.] National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>.
- [25.] OECD. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD.
- [26.] OECD. (2025). AI adoption by small and medium-sized enterprises. OECD Publishing.
- [27.] Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation-augmentation paradox. *Academy of Management Review*, 46(1), 192-210. <https://doi.org/10.5465/amr.2018.0072>.
- [28.] Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency*, 33-44. <https://doi.org/10.1145/3351095.3372873>
- [29.] Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- [30.] Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. Irwin/McGraw-Hill.
- [31.] Sterman, J. D. (2002). *System dynamics: Systems thinking and modeling for a complex world*. Massachusetts Institute of Technology.
- [32.] Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. *Strategic Management Journal*, 28(13), 1319-1350. <https://doi.org/10.1002/smj.640>.
- [33.] Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z).
- [34.] Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
- [35.] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. <https://doi.org/10.2307/30036540>.
- [36.] Wamba-Taguimdje, S. L., Wamba, S. F., Kamdjoug, J. R. K., & Wanko, C. E. T. (2020). Influence of artificial intelligence on firm performance: The business value of AI-based transformation projects. *Business Process Management Journal*, 26(7), 1893-1924. <https://doi.org/10.1108/BPMJ-10-2019-0411>.