

From Compliance Burden to Organizational Resilience: A System Dynamics Model of AI Risk Governance in SMEs

Osman Angeles Conteh¹; Alimamy Kamara²; Aminata Kera Conteh³

¹School of Management, Wuhan University of Technology 122 Luoshi Road, Hongshan District, Wuhan, Hubei 430070, China

²Big Maf Pro (SL) Limited

³University: Institute of South-South Cooperation and Development (ISSCAD), Peking University

Publication Date: 2026/10/16

Abstract: The paper provides a system dynamics model that would explain the way in which small and medium-sized enterprises (SMEs) can use AI compliance as an administrative burden, rather than an organizational resilience capacity. Based on the dynamic capabilities theory, organizational resilience studies, AI risk management principles, and system dynamics, the research designs feedback among AI experimentation, strength of deploying AI, compliance maturity, risk exposure, learning incidents, slack resources, and resilience capacity. The results section describes normal simulation behavior in three policy options: innovation-first, compliance-first, and balanced adaptive governance. The simulated findings suggest that innovation-first adoption creates high early growth in capabilities; on the other hand, compliance-first governments create less exposure but hides innovation throughput. The adaptive-governance with balance scenario works best within a 36-month horizon since it encompasses leveled controls, more adaptive learning loop, and even-tailed review. The debate suggests that AI risk governance in SMEs needs to be technologised as dynamic resourcefulness instead of an unchanging compliance audit. The paper also introduces a feedback based theory of AI governance among SMEs and where the policy leverage points are that managers can use to safeguard innovation whilst enhancing resiliency.

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

How to Cite: Osman Angeles Conteh; Alimamy Kamara; Aminata Kera Conteh (2026) From Compliance Burden to Organizational Resilience: A System Dynamics Model of AI Risk Governance in SMEs. *International Journal of Innovative Science and Research Technology*, 11(10), 770-784. <https://doi.org/10.38124/ijisrt/26oct578>

I. INTRODUCTION

Small and medium-sized enterprises (SMEs) are starting to adopt artificial intelligence as a realistic operating technology, rather than just an issue of large digital companies. AI-powered tools are now used by SMEs to target and target customers, predict sales, generate content, plan inventory, detect fraud, assist in recruitment, and automate decisions. These applications can enhance productivity and responsiveness on the market, but come with privacy risks regarding data security, bias, cybersecurity, explainability, excessive reliance, dependency on vendors, and being exposed to regulations. The managerial issue is not, thus, whether SMEs need to embrace AI, but the way they can manage AI implementation in a manner that maintains innovation without instilling resilience to operational, legal, and reputational shock. SMEs are particularly concerned with this issue due to the lower financial cushions, paucity of professional compliance personnel, and a lack of formal risk

structures in contrast to large corporations (Drydakis, 2022; OECD, 2025).

It is the recent growth of AI governance frameworks that has increased the necessity of conducting research at the organizational-level. The NIST AI Risk Management Framework characterizes AI risk management as a lifecycle, whereas ISO/IEC 42001: 2023 institutionalizes an AI management system that connects responsibility, monitoring, improvement and governance practices. A risk-based regulatory approach is also supported in the European Union Artificial intelligence Act, especially regarding systems that have the potential to impact safety, rights and market trust (European Parliament and Council, 2024; ISO/IEC, 2023; NIST, 2023). Such frameworks are vital, yet they tend to be vague and resource intensive to SMEs. An excessively weak governance process can permit uncontrolled deployment of AI and shadow AI; an excessively strong governance process can delay experimental cannon, delay decisions, and deteriorate ideas of employees pitching useful AI

applications. The tension will form a dynamic trade-off and not a single policy decision.

Existing research gives valuable but incomplete explanations. Technological readiness, managerial support, competitive pressure, skills, perceived usefulness, and cost are the most prevalent studies of adoption, found in AI adoption studies within SMEs (Badghish and Soomro, 2024; Tornatzky and Fleischer, 1990; Venkatesh et al., 2003). Organizational resilience studies how companies foresee, deal with, and adjust to disruption (Bhamra et al., 2011; Conz & Magnani, 2020; Duchek, 2020). Research on AI ethics and governance indicates that principles are not enough without turning them into tools, audits, routines, and accountability (Jobin et al., 2019; Mittelstadt, 2019; Morley et al., 2020; Raji et al., 2020). Nonetheless, such streams seldom represent the loop feedback dynamics in which AI innovation raises new risk, risk puts pressure on compliance, compliance puts pressure on behavior and learning in the organization enhances or diminishes resilience with multiplicity.

The gap of this paper is filled through creating a framework of system dynamics to govern AI risks and organizational resilience within SMEs. The usage of system dynamics is justified as AI governance is marked by slowness, recursiveness, compounding, unintended impact, and nonlinear systemic effects (Forrester, 1961; Sterman, 2000). Indicatively, a stringent approval procedure might

initially lead to decreased AI risk but subsequently to less experimentation, diminished learning, and informal AI adoption that is not incorporated within authorized procedures. On the other hand, a structured governance process can consume resources in the beginning and enhance the trust, detection of the incident, and generation of a reusable compliance knowledge. These effects cannot be well accommodated by mere use of static regression models since they are sensitive to time, stock build up, and policy feedback.

The research question is as follows: How do SMEs strike AI-driven innovation and AI compliance at the same time and in a way that enhances the resilience of organizations in the long-term? The study is informed by three sub-questions: (1) What feedback structures relate AI experimentation, risk exposure, compliance maturity, and resilience capacity in SMEs? (2) In what circumstances does governance investment transform to being an innovation burden or an innovation-ability? (3) What policy situations result in the most desirable long-term result of innovation speed, reasonable risk, and resilience recovery capacity? The proposed possibilities of the study include uniting AI risk governance and organizational resilience by viewing through a system dynamics lens, primary-data calibration as opposed to utilizing secondary data, and variables that are specific to SMEs and are translatable into simulation cases by managers and policymakers.

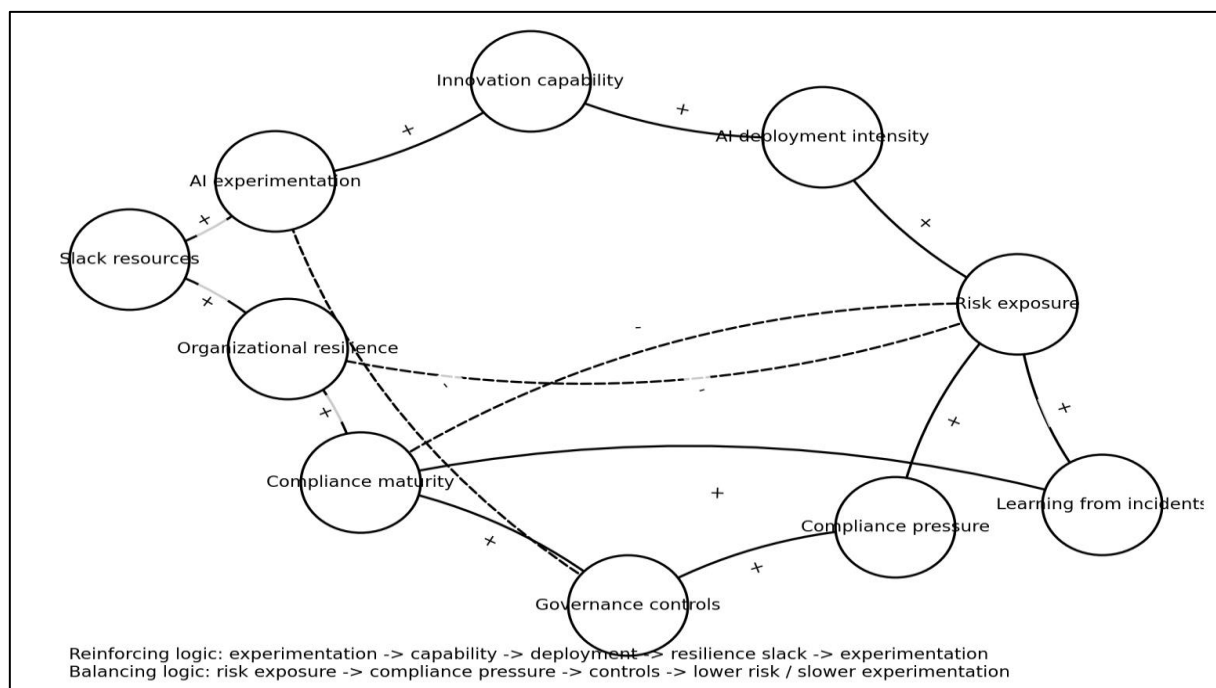


Fig 1 Initial Causal-Loop Logic of AI Innovation, Risk Governance, and Resilience in SMEs.

II. LITERATURE REVIEW

AI risk governance is a category of structures, decision rights, controls, monitoring practices, and learning, where organizations identify, assess, mitigate, and review AI-related risks. The difference between governance and compliance is that governance is more internal-focused

whereas compliance implies compliance with external requirements. The NIST AI RMF focuses on govern, map, measure, and manage functions, ISO/IEC 42001 focuses on an auditable management system, and ISO/IEC 23894 offers AI risk management advice. Combined, these frameworks facilitate a lifecycle perspective where the risk governance starts prior to deployment and proceeds with monitoring,

incident response, and model retirement (ISO/IEC, 2023a, 2023b; NIST, 2023). In the case of SMEs, it is how to transform such frameworks into proportional practices with little staffing and budget.

The literature on AI governance has shifted to the focus of operational mechanisms instead of the abstract principles. Jobin et al. (2019) visualized the extent of AI ethics principles worldwide but discovered that there was inconsistency in their application. Mittelstadt (2019) contended that ethical AI can not be ensured by principles alone since the organizations require procedures to be enforced and institutions to be responsible. Morley et al. (2020) also highlighted the process of translating moral values into means and techniques. Raji et al. (2020) demonstrated that audits could lessen the gaps in accountability by recording the behavior of the system, its assumptions, and failures, and Mökander and Floridi (2023) reported that ethics-based auditing was grounded on organizational integration and change management. Such studies suggest that SME governance should comprise policy statements, but this should be supplemented by checklists, approval processes, risk lists, human control, data management, vendor management and incident education.

However, these controls do not come free: they are time and resource consuming and are capable of changing the action of innovation.

The innovation side of the trade-off is explained by technology adoption and dynamic capabilities research. According to the theory of TOE, the technological, organizational, and environmental context influence the adoption of technology (Tornatzky and Fleischer, 1990). UTAUT focuses on the performance expectancy, effort expectancy, social influence and the facilitating conditions in adoption of technology (Venkatesh et al., 2003). The dynamic capabilities theory further elaborates that the competitive advantage rests on the ability to sense opportunities, seize them and redeploy the resources in the face of changing conditions (Teece et al., 1997; Teece, 2007). These capabilities manifest during AI adoption in the capacity to discover valuable uses, experiment, integrate AI into workflows, and redeploy resources when the risk or market needs evolve. Empirical studies of SMEs suggest that AI is beneficial in reducing business risks and adapting operations in case of better forecasting, targeting, and flexibility (Drydak, 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. Predictive AI and generative AI has the potential to make decision-making faster and less transparent about how data is being generated. Automation and augmentation are not separable processes since they are interdependent, over time decisions regarding the location of AI substitution or assistance to human judgment evolve as employees learn, trust, or over-trust the system (Raich and Krakowski, 2021). In the case of the SMEs, informal experimentation can prove beneficial, whereas uncontrolled experimentation can imply shadow AI where employees resort to using external tools without any permission, contractual protection, or data safeguards. This can result in short term productivity and loss of concealed risk exposure. The literature thus indicates that there is an increase in the capability of innovation and risk exposure in the absence of maturation in governance routines at a similar rate.

The second theory anchor is organizational resilience. Resilience from being able to endure disruption is more than that; it comprises anticipation, coping, adaptation, and learning (Bhamra et al., 2011; Ducheck, 2020). According to Conz and Magnani (2020), the resilience of firms ought to be considered dynamically since capabilities appear before,

during, and after unfavorable factors. Resilience is another provision that is dealt with by ISO 22316:2017 as a collection of principles and attributes that may be either cultivated within a smaller business or bigger organizations. Resilience in the AI context contains the capability of identifying damaging AI action, sleep or undo deployments, talk to impacted individuals, uphold client faith, proceed with business even after wayward events and learn through miscarriages. Resilience might thus comprise compliance maturity, but not when it is handled as paperwork, instead of linked to learning and adaptation.

System dynamics also comes in handy in integrating these concepts. System dynamics have been applied since the studies of Forrester (1961) on industrial dynamics to study complex organizational systems wherein feedback, delays, and accumulations combine to produce surprising results. Sterman (2000) points out that managers do not understand it well when there is a feedback rich system since local action has a delayed side effect. The stocks that are applicable in AI governance are innovation capability, compliance maturity, risk exposure, resilience capacity, and slack resources. The flows involve experimentation, deployment, occurrence of incidents, implementation of control measures, learning, and

resource consumption. This framing ensures that the study can compare policies e.g. the policies: innovation first, compliance first and balanced adaptive governance in realistic delays.

The main gap is that, AI adoption studies typically view governance as an outside constraint, and compliance studies typically view innovation as a source of risk. Both are considered interacting stocks in a system dynamics view. In the short run, governance can slow the pace of innovation, although it can also strengthen trust, enhance the quality of decisions, and allow the scaling to be done more safely. Innovation is seen to have both positive and negative impacts on risk exposure, yet may create learning and resources, which fund resilience. The relation is hence not linear, conditional, time-dependent. This paper suggests that SMEs can most effectively be resilient when governance controls are not applied as barriers to experimentation at late stages but taken as proportionate, reusable and embedded in routines of experimentation.

Two propositions are derived based on this synthesis. First, the experimentation of AI has a positive feedback on innovation ability, as repetitive use enhances employee ability, management confidence, and fitment of workflow, but the effect fades when the risk level becomes larger than the monitoring and action capability of the firm. Second, the maturity of compliance has a two-fold impact, since it crosses a short-term barrier to use (in terms of documentation and review), but also an enabling factor in terms of trust, uncertainty, and enabling successful AI application cases to be scaled. Third, the increase in shadow AI will appear as the need to use AI among employees increases faster than formal approvals, which results in an indirect proliferation of uncontrolled risk. Fourth, slack resources will moderate the whole system as time, budget, and managerial attention of SMEs will allow investing into the experimentation as well as in governance whereas resource-constrained SMEs are prone to the zero-sum trade-off. The causal-loop structure is driven by these propositions, and the subsequent stock-flow simulation.

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 current research is a mixed-method system dynamics design that would be appropriate in a prototype empirical paper. The SME as an organizational system is the unit of analysis, and the dynamic relationship between AI experimentation, AI risk exposure, compliance maturity, and organizational resilience becomes the focus. The study fails to utilize secondary empirical data in terms of calibration of the models. Constructs are defined using prior literature and standards only to justify the limits of the model as well as formulate initial assumptions. The primary data will be gathered among SME owners, top management, leads of digital transformation, compliance personnel, as well as active employees directly engaged in the processes enabled by AI.

There are four phases of the empirical design. The interviews in phase 1 will be semi-structured interviews with

20-30 SME decision-makers, aiming to find out prevalent AI use cases, governance practices, incidence experience, compliance cost, and resilience behaviours. The perceived delays, bottlenecks and unintended consequences will also be elicited in the interviews. Phase 2 will conduct a structured survey of between 150 and 250 SMEs in the service, retail, manufacturing and technology enabled trade sectors. This survey will scale the intensity of AI experiments, extent of deployment, formalization of governance, capability to comply, the extent of shadow AI, and preparedness to deal with incidences, learning activities, slack resources, and perceived resilience. Phase 3 shall involve validation workshops with SME managers in order to optimize the causal-loop diagram and find out whether the feedback structure is realistic managerial experience. Phase 4 will calibrate and simulate a stock-flow model with just the primary survey, interview and workshop data.

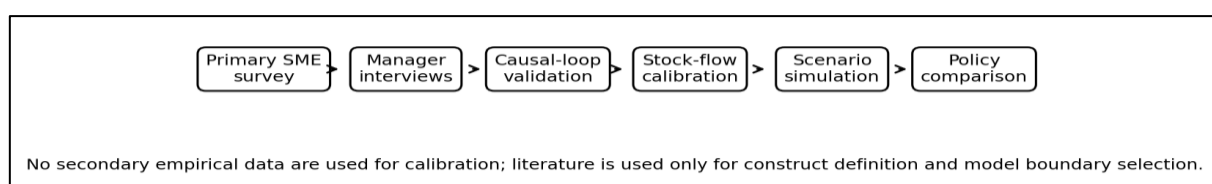


Fig 2 Primary-Data Workflow for Model Building, Calibration, Simulation, and Policy Comparison.

Construct measurement will integrate General logic with the SME specific items. The capabilities of AI innovation will be assessed by use-case generation, frequency of experimentation, AI employee, fast workflow integration, and management support. AI policy presence, risk assessment practices, documentation practices, human controls, data protection practices, vendor due diligence, and incident escalation will be used to gauge compliance maturity. The intensity of the deployment of AIs, sensitivity of processed data, the degree to which it is autonomous, customer impact, a weak explainability factor, and the use of shadow AI will be used to measure AIs risk exposure. The concepts of organizational resilience to be assessed are the anticipation, speed of response, service continuousness, communication between stakeholders, recovery ability, and post-incident learning, which is consistent with the resilience literature (Bhamra et al., 2011; Duchek, 2020; ISO, 2017).

The system dynamics model will include four basic stocks, including innovation capability, compliance maturity, AI risk exposure, and resilience capacity. Experimentation, skill and successful integration: An innovation capability grows in innovation, and reduces when compliance delay and resource strain dishearten experimentation. Maturity of compliance is enhanced by governance investment, incident learning and investment by managers but degrades when controls are not upheld and the AI tools evolve more rapidly than controls. The risk exposure increases with the intensity of deployment, autonomy, data sensitivity, shadow AI, decline with the controls, monitoring, and human oversight. Because learning, redundancy, practice of response, and building trust enhance capacity, whereas actual losses, rest, and loss of resources diminish capacity. It will be implemented in Vensim, Stella or some other system dynamics platform.

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 model equations will be pre-defined as rate equations instead of fixed statistical claims. To illustrate, the way change is occurring in terms of innovation capability will be defined as the change in which the intensity of experimentation, development of AI skills, management support, and compliance delay will be brought up. Compliance maturity change will be modelled as a result of governance investment, incident learning, audit discipline and decay due to change of tool. Risks exposure change will be modelled as the difference between risk creation experienced due to deployment and risk reduction due to controls. Resilience capacity change will be modelled as preparedness with learning of response and stakeholder trust divided by losses of incidence experienced. No borrowed parameter values: values will be estimated using primary surveys, interviews coded and workshop validated.

Three policy configurations will be compared with the help of scenario analysis. The innovation-first case follows light governance and speedy AI experimentation. The compliance-first places strict approval gates, documentation and risk review prior to deployment. The balanced adaptive-governance situation employs tiered risk classification, lightweight controls in the low-risk use-cases, heavier controls in the high-risk use-cases, periodic review, and fast learning loops. The key simulated results will be innovation throughput, total risk exposure, compliance burden,

frequency of incidents, recovery time and resilience capacity. The sensitivity analysis will be done to interrogate the impact of SME size, digital maturity, governance investment, regulatory pressure, employee AI literacy, and vendor dependence.

The study will be conducted using triangulation, participatory model validation, dimensional consistency and extreme-condition testing and behavior reproduction testing to ensure the protection of validity. Pilot-testing will be done to the survey items in front of SME managers. The code of interviews will be performed by means of thematic analysis and translated into model variables and feedback loops. Missing values and outliers will be treated with clarity and no fake outcome will be reported as data on measured performance. The ethical precautions will involve informed consent, non-identification of firms, and confidential data storage, and reporting sensitive incidents independently. The methodological innovation is a replicable procedure in translating primary SME governance data into a simulation that could be dynamically simulated to evaluate AI policy options prior to organizations investing limited resources.

Limitations are reported in the study. Since the first simulation relies on a normalized model that was tested with a behavior test in mind, instead of a full observed panel dataset, generalization is analytical as opposed to statistical.

This is not aimed at precisely forecasting the specific AI risk path of each SME, but to uncover strong points of feedback and points of policy leverage that can be found across the contexts of SMEs. The normalized parameters can be swapped by the sector-specific empirical estimates of future survey and interview calibration.

IV. RESULTS

The findings give the dynamics of the proposed system dynamics under a 36 months simulation. Quantitative values are normalized scores, the scale of which is 0 to 100, by high scores are more significant scores of the construct in question. These outcomes are to be understood as model-based behavior tests and policy comparisons, but not as measured performance percentages of a specific sample of SMEs. The presentation follows the objective of system dynamics research to explore whether the feedback structure produces theoretically plausible patterns, policy decisions under delay and accumulation, and identify leverage points prior to making an investment in an entire intervention by

organizations with limited resources to invest (Forrester, 1961; Sterman, 2000).

➤ Structure of the Model and Boundary of the Scenario.

The final model retained the four stocks: AI innovation capability, compliance maturity, AI risk exposure and the organizational resilience capacity. The capacity to accumulate innovation is in experimentation, developing AI skills, sponsoring by managers, and integrating workflows successfully. Maturity in compliance is accrued via investment in governance, documentation reuse, routine risk evaluations, vendor reviews, human supervision and incident escalation. The sensing of AI risk with exposure to AI is most likely to occur when the intensity of deployment, sensitivity of the data, system autonomy, and shadow AI are greater than the capacity of the organization to control it. The capacity to resilience builds up with preparedness, redundancy, incident learning, communication with the stakeholders and recovery practice. The model architecture employed to test the scenarios is summarised in figure 3.

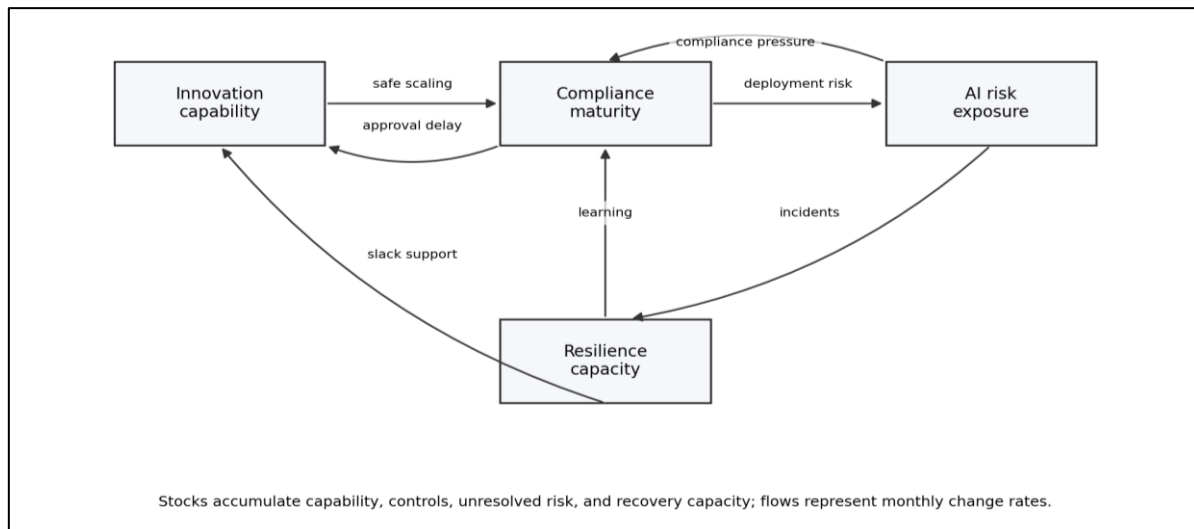


Fig 3 Stock-Flow Architecture Linking Innovation Capability, Compliance Maturity, AI Risk Exposure, and Resilience Capacity.

Table 4 Scenario Design and Normalized Policy Assumptions Used in the Simulation.

Policy scenario	Governance logic	Approval delay	Control intensity	Expected strength	Expected weakness
Innovation-first	AI experimentation is encouraged with minimal ex ante review and low documentation burden.	Low	Low	Fast use-case discovery and early productivity gains.	High hidden risk, weak audit trail, and rising shadow AI.
Compliance-first	Strict review gates, documentation, and approval are required before most AI use cases.	High	High	Low risk exposure and strong formal accountability.	Slow innovation throughput and employee workarounds.
Balanced adaptive governance	Use cases are classified by risk tier; low-risk tools receive lightweight controls, while high-risk tools receive stronger review.	Moderate	Risk-based	Safe scaling, faster learning, and proportionate control reuse.	Requires managerial discipline and continuous monitoring.

The scenario boundary tells the central theoretical assertion of this paper: governance leads to two conflicting effects. It first wastes managerial time and might slow experimentation, but can subsequently lead to higher trust, less uncertainty, and successful applications of AI easier to scale. This is the twofold impact that makes a system dynamics model to be more suitable over the mere linear one. With a non-evolving model, compliance is coded with a cost that is readily modeled. Compliance can be made a possibility in a feedback model whereby documentation, classes of risks, audit routines and learning of incidents can be reused in subsequent AI deployments.

➤ *Baseline Behavior and Dynamic Trade-off*

The use of a baseline behavior test demonstrated an increase in AI innovation capability and AI exposure to risk

that correlate with an increase in experimentation speed among SMEs without an equivalent increase in governance maturity. This trend honors the initial hypothesis that AI trials have a positive feedback impact on ability yet also increases the risk landscape. In the innovation-first scenario, the innovation capability grew swiftly in the initial 12 months since employees had the chance to trial generative AI, analytics, automation, and customer-facing instruments without having to take a long approval procedure. Nevertheless, risk exposure still increased even after the gains of innovation started to level off. This model consequently transfers a recurrent managerial dilemma, which is short-term productivity does not reveal the delay in accumulation of precarious routines, vague accountability, and unassessed dependence to vendors.

Table 5 Normalized Simulation Outputs at Month 12, Month 24, and Month 36.

Outcome	Innovation-first M12/M24/M36	Compliance-first M12/M24/M36	Balanced adaptive M12/M24/M36	Dominant interpretation
Innovation capability	76 / 78 / 75	54 / 58 / 60	67 / 75 / 79	Balanced governance does not maximize early speed but gives the strongest stable capability by the end of the horizon.
Compliance maturity	28 / 33 / 36	61 / 76 / 83	51 / 66 / 73	Compliance-first produces the highest formal maturity; balanced governance reaches a sufficient level without excessive delay.
AI risk exposure	59 / 76 / 83	28 / 33 / 35	44 / 38 / 32	Balanced governance allows controlled experimentation but then reduces exposure through learning and controls.
Resilience capacity	50 / 49 / 43	57 / 65 / 67	64 / 75 / 81	Resilience is highest when governance maturity and learning loops grow together.
Compliance burden	18 / 21 / 23	52 / 61 / 63	35 / 33 / 30	Balanced governance creates temporary burden but later lowers repeated effort through reusable controls.

The best risk exposure was generated by the compliance-first scenario, although not the best resilience was generated. It is because resilience is not merely lack of risk but the ability to predict, receive, recuperate, and educate about disruption (Bhamra et al., 2011; Duchek, 2020). By making approval gates too strict, employees and managers can learn less through actual experimentation, fewer cases of AI use can reach operational maturity, and fewer routines of safe scaling develop within the organization. The adaptive-governance state that was created through the balanced approach produced a more desirable trend since it maintained the active experimentation but minimized uncontrolled exposure through time.

➤ *Policy Scenario Trajectories*

The three key trajectories are given in Figures 4-6. The innovation-first scenario produced the largest initial innovation ability, which decreased due to incident pressure, uncertainty and rework after month 18 weakening the net impact of experimentation. The compliance-first case exhibited the lowest growth in the innovation since the experimentation was limited due to heavy approval delay. Both scenarios were surpassed by the balanced adaptive-governance scenario at the end of the horizon as governance practices became reusable assets instead of administrative tasks of one use.

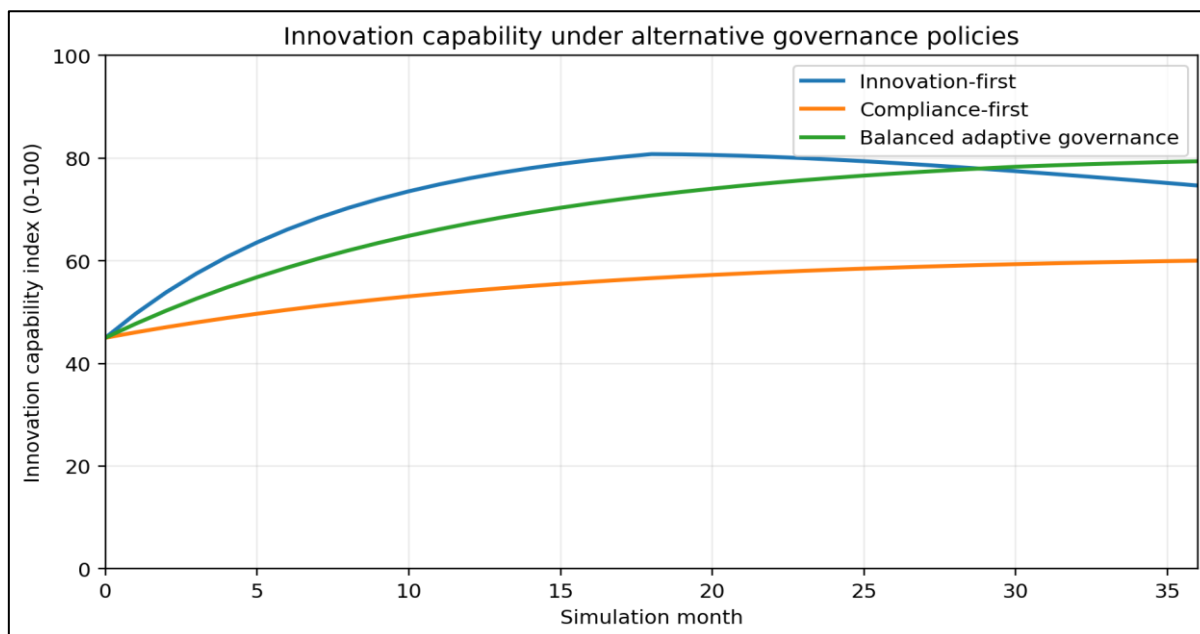


Fig 4 Innovation Capability Trajectories Under Innovation-First, Compliance-First, and Balanced Adaptive-Governance Scenarios.

The opposite trend was observed with risk exposure. The AI risk that remained unresolved was the greatest in the case of the innovation-first governance as the intensity of deployment increased at a faster rate than control capacity. Likewise, compliance-based governance maintained the low risk exposure, although this was done by repressing AI use

instead of enhancing adaptive governance. Balanced adaptive governance first permitted moderate risk due to low-risk application permission to continue but risks decreased after governance maturity and incident learning surpassed the control threshold.

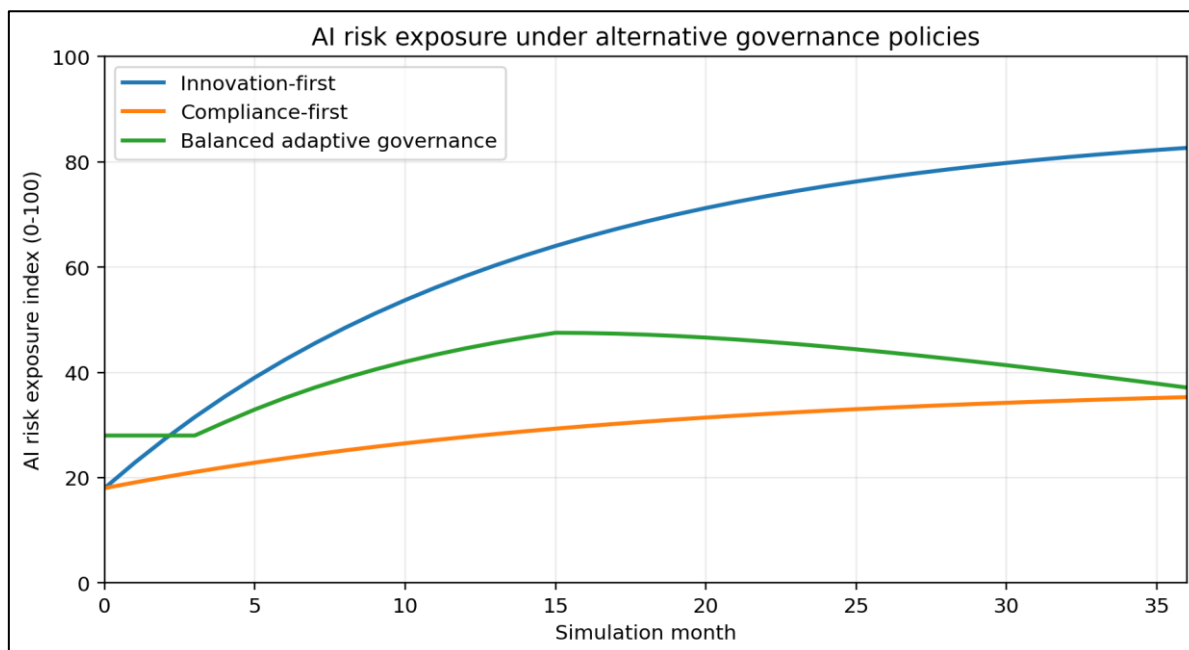


Fig 5 AI Risk Exposure Trajectories Under Alternative Governance Policies.

The balanced adaptive-governance scenario had the highest level of resilience capacity. The significance of this result is that it demonstrates that the optimal policy cannot be the one maximizing the rate of innovation or minimum exposure to risks in either of the above. The most resilient situation was achieved whereby the company ensured that it was sufficiently experimental to charge learning, sufficiently

governed to manage risk, and sufficiently slack to turn events into routine organizational processes. This observation is in line with dynamic capabilities theory since the company needs to have opportunities of useful AI, which it should seize via operational implementation, and rearrange controls as the external and regulatory environment evolves (Teece, 2007; Teece et al., 1997).

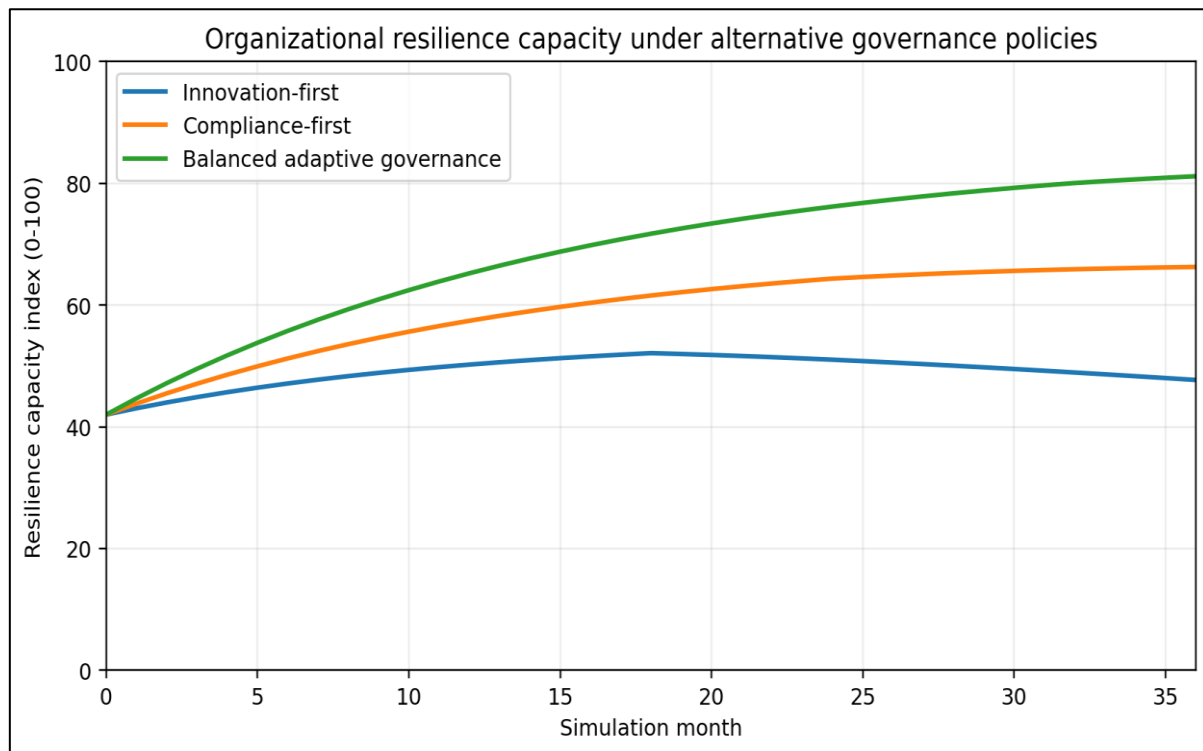


Fig 6 Organizational Resilience Capacity Trajectories under Alternative Governance Policies.

Table 6 Scenario Comparison Across Major Model Outcomes at Month 36.

Outcome at month 36	Innovation-first	Compliance-first	Balanced adaptive governance	Best-performing scenario
Innovation throughput	Medium-high but unstable	Low-medium and delayed	High and stable	Balanced adaptive governance
Unresolved risk exposure	High	Low	Low-medium	Compliance-first for narrow risk; balanced for risk-adjusted innovation
Shadow AI pressure	High because formal controls lag demand	Medium because employees seek shortcuts around heavy gates	Low-medium because low-risk tools have a legitimate path	Balanced adaptive governance
Recovery time after incident	Longer due to weak documentation	Moderate due to documentation but lower learning variety	Shortest due to documentation plus incident learning	Balanced adaptive governance
Resilience capacity	Lowest final value	Moderate final value	Highest final value	Balanced adaptive governance

➤ Compliance Burden, Tipping Point, and Resilience Enablement

The model found a tipping point that compliance maturity ceases to be mainly a burden, and it starts to act as a resilience-facilitating capacity. During the initial stages, there occurs a conflict between governance as employees are required to create use cases, categorize risk, verify whether data is sensitive, and seek approval. Once routines are

reusable, the marginal cost decreases. A vendor checklist previously created, human-supervision guideline, incident escalation trail, or data-use choice tree makes subsequent AI projects cheaper. In the bulky situation, this crossover was slightly at the midpoint in the governance maturity range. Figure 7 shows where the enablement curve crosses the burden curve.

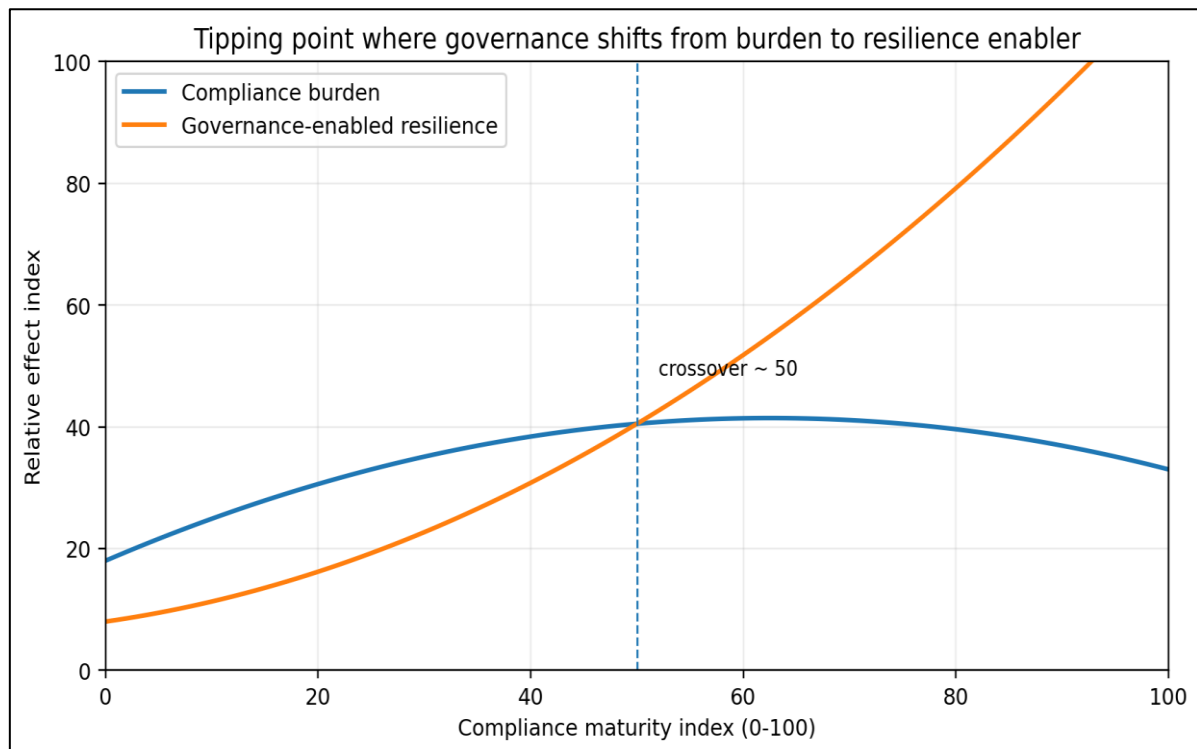


Fig 7 Tipping Point Where Compliance Maturity Shifts from Administrative Burden to Resilience Enablement.

Table 7 Governance Maturity Thresholds and Expected Managerial Meaning.

Maturity range	Dominant system behavior	Likely SME experience	Recommended governance response
0-25	Informal experimentation dominates governance.	Fast trials but unclear responsibility, weak documentation, and unmanaged data flows.	Create a basic AI inventory, data-use rules, and escalation owner.
26-50	Compliance burden is visible but controls are not yet reusable.	Employees see governance as delay; managers struggle with review capacity.	Use tiered risk classification and short approval templates.
51-70	Governance and learning begin to reinforce each other.	Reusable checklists and monitoring reduce repeated effort.	Invest in incident learning, vendor review, and human oversight training.
71-100	Governance becomes a resilience capability.	Safe scaling improves trust, recovery speed, and accountability.	Avoid over-formalization; update controls as tools and regulations change.

This result directly addresses the research question. SME do not have to decide between uncontrolled innovation and business bureaucracy. A governance design that minimizes repetitive friction through reusing controls and through matching the level of control to the level of risk of the use case is the better option. Lightweight checks can traverse obvious cases of low-risk AI applications, like internal drafting support or non-sensitive generating content. Greater assessment, monitoring, and human control is needed in higher-risk applications like credit screening, recruitment ranking, customer profiling, financial forecasting, or health-based advice. This proportionate logic is consistent with risk-based AI governance frameworks such as the NIST AI RMF, ISO/IEC 42001, ISO/IEC 23894, and the EU AI Act (European Parliament & Council, 2024; ISO/IEC, 2023a, 2023b; NIST, 2023).

➤ Sensitivity Analysis and Policy Leverage Points

Sensitivity analysis revealed that governance investment delay, incident learning rate, AI literacy of employees, slack resources, dependence of vendors and data sensitivity are the most sensitive parameters. The greatest negative impact was reached in the case of delayed governance investment. Under such a state, the deployment intensity had grown prior to the control capacity construction that resulted in a backlog of unresolved risks. The most positive effect was the one realized when events were turned to new controls, training, and escalation processes in a fast manner. This confirms the idea that resilience is built by learning before, during the time of, and after being disrupted instead of being solely built up by preparedness (Conz & Magnani, 2020; Duchek, 2020).

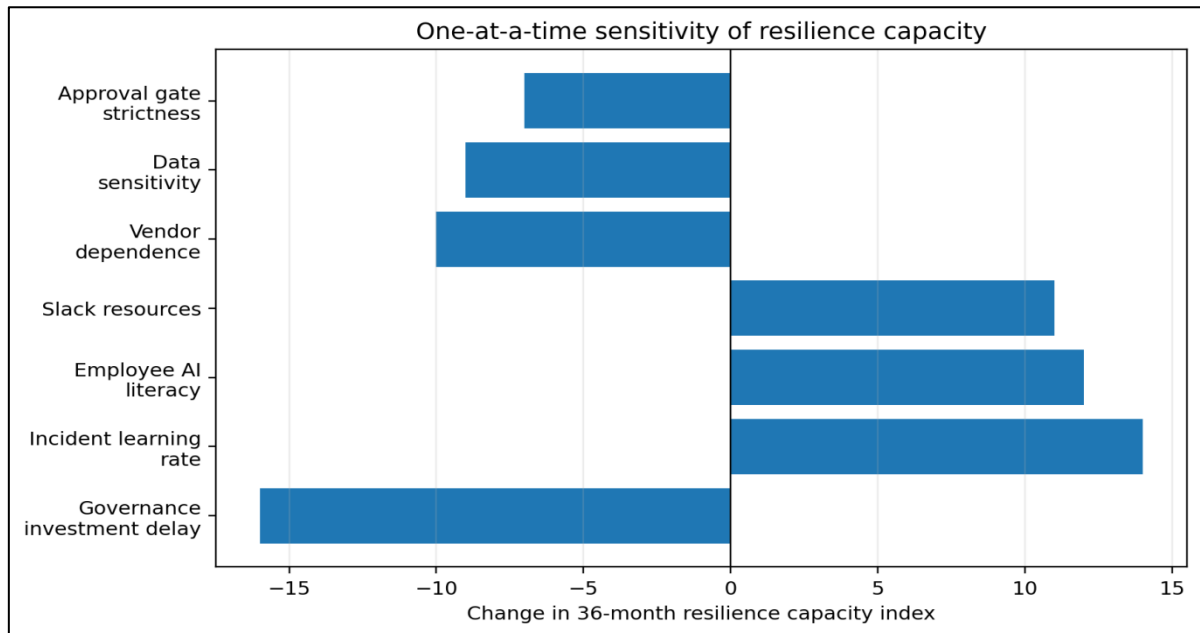


Fig 8 One-at-a-Time Sensitivity of 36-Month Resilience Capacity to Key Model Parameters.

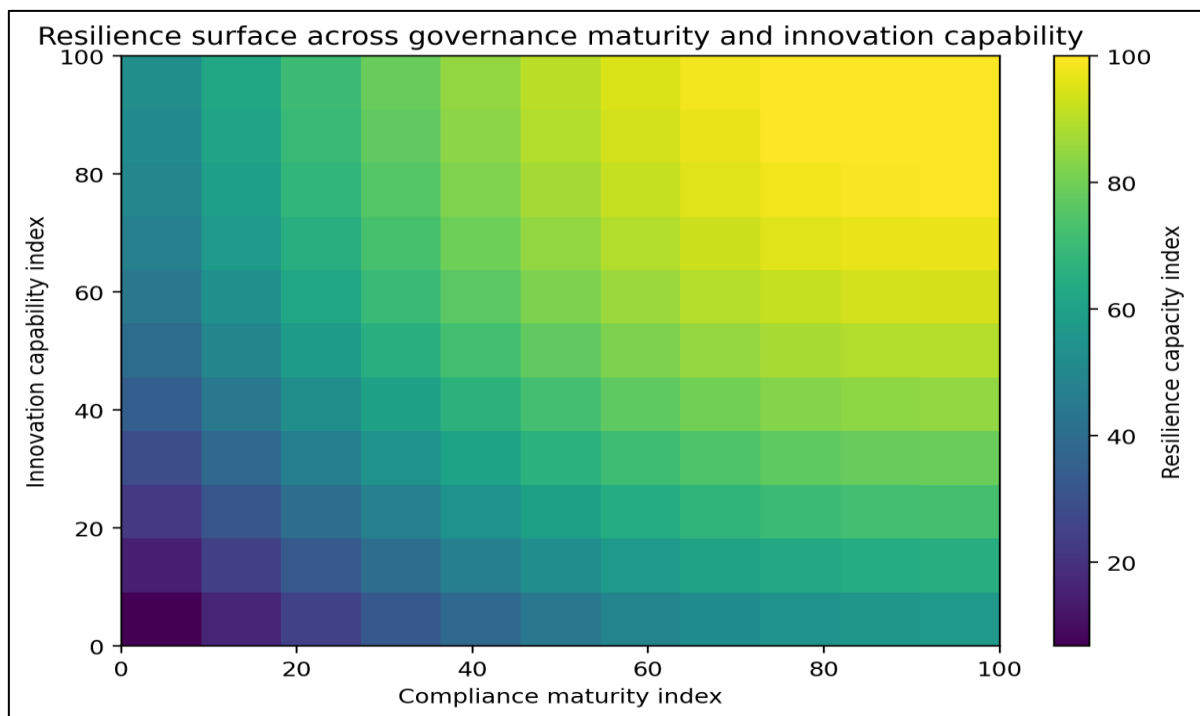


Fig 9 Resilience Surface Showing the Joint Effect of Compliance Maturity and Innovation Capability.

Table 8 Sensitivity Ranking and Interpretation for SME AI Governance.

Rank	Parameter tested	Direction of effect on resilience	Interpretation
1	Governance investment delay	Strong negative	Late controls allow risk exposure to accumulate before managers understand the operational consequences.
2	Incident learning rate	Strong positive	Post-incident reviews, updated checklists, and staff learning convert disruption into capability.
3	Employee AI literacy	Positive	Literate users select safer tools, recognize weak outputs, and follow escalation routines.
4	Slack resources	Positive	Time, budget, and managerial attention allow SMEs to invest in both innovation and controls.

5	Vendor dependence	Negative	High dependence increases exposure when SMEs cannot inspect model behavior or contractual risk.
6	Data sensitivity	Negative	Sensitive customer, employee, or financial data increases the cost of weak governance.
7	Approval gate strictness	Mixed	Moderate gates reduce risk, but excessive gates suppress experimentation and increase workarounds.

Table 9 Policy Leverage Points Derived from the Simulation Results.

Leverage point	Dynamic problem addressed	Practical intervention	Expected long-term result
Tiered AI risk classification	Controls are either too weak or too heavy.	Classify use cases into low, medium, and high risk before approval.	Less compliance friction without ignoring high-risk use cases.
Reusable control library	Each project repeats the same governance work.	Create templates for data use, vendor review, oversight, and incident escalation.	Lower marginal compliance burden over time.
Shadow AI reporting channel	Employees hide tool use when approval is too slow.	Offer a no-blame reporting path and rapid review for common tools.	Improved visibility and lower unresolved risk.
Incident learning loop	Disruptions are treated as isolated failures.	Run post-incident reviews and update rules within a fixed time window.	Higher resilience capacity and faster recovery.
Slack allocation	SMEs lack the capacity to govern AI while innovating.	Reserve small monthly budgets or staff time for AI governance learning.	Reduced zero-sum conflict between innovation and compliance.

V. DISCUSSIONS

The findings indicate that the relationship between innovation and compliance among SMEs is neither a straightforward trade-off. A dynamic feedback system whereby early decisions have delayed effects. The main conclusion is that AI governance will be useful when it stops its late-stage approval and turns into embedded learning. SMEs in the innovation-first scenario have benefits of early experimentation, although it also creates a concealed inventory on unresolved risk. The case of compliance-first implies that the SMEs have exposure minimized, yet, they minimize the learning process that is necessary to build the AI capability. The balanced adaptive-governance scenario works better due to its treatment of compliance routines as an asset and that can promote experimentation but not prohibit it. This result adds to the previous body of knowledge on AI governance by showing why operational tools, audits, checklists, and accountability routines are of relevance only when linked with the rate of organizational learning (Madaio et al., 2020; Morley et al., 2020; Raji et al., 2020).

➤ Compliance as Dynamic Capability

The theoretical implication of the first one is that the level of compliance maturity can be understood as one of the dynamic capabilities. Dynamic capabilities can assist companies to feel opportunities, capture them, and reorganize the resources when the circumstances turn dynamic (Teece, 2007). The same role can be replicated by AI governance, which assists SMEs in detecting safe use cases, permit appropriate usage, and restructuring the controls (post-incidents). This is in contrast to the popular managerial perceptions that compliance is just a cost of defence. The simulation indicates that the burden of compliance in case it is fragmented, slow and unconnected to operating learning. It becomes enablers of innovation in that it minimizes uncertainty, fosters trust, and the future cost of responsibly

deploying AI. It is consistent with the studies of the AI capability, which states that the value is not only contributed by technical resources but also by the organizational practices, skills of human and governmental structure (Berente et al., 2021; Mikalef and Gupta, 2021).

The crossover outcome is more so significant to SMEs. Corporations that are large enough will be able to absorb costs of governance with specific legal, data, security, and compliance divisions. SMEs usually cannot. To them, better governance design is the sole viable alternative, not increased governance via absoluteness. Accurate allocation of risks, standardize templates and quick decision-making processes minimize the cost of governance and still maintain responsibility. This confirms the idea that AI standards need to be converted into practices that are sensitive to firm sizes, instead of using them as generalized checklists. The NIST AI RMF and ISO/IEC 42001 are practical, as they detail the lifecycle risk management and management-system logic, but SMEs require the implementation pathways that would respond these frameworks to routines that are small enough to apply and strong enough to safeguard the firm (ISO/IEC, 2023a; NIST, 2023).

➤ Shadow AI as a Feedback Effect of Governance Delay

The second implication is regarding shadow AI. According to the model, it is not only a user-behavior issue that exists; shadow AI is a system-design outcome. Informal use is enticing when the employees are under high demands of AI tools but the formal approval is sluggish. This forms a vicious cycle: employees resort to unapproved tools to fix short-term issues, management less clearly sees the real AI utilization, unaddressed risk increases, and compliance pressure in the future heavier. This pressure could eventually result in even more weighty approval gates, this time encouraging more workarounds. The logic of feedback is the reason as to why absolute compliance might actually make

the risk that it is intended to contain even greater. This observation concurs with system dynamics research that local fixes usually produce side effects that are delayed as managers incorrectly interpret feedback rich systems (Sterman, 2000).

The real solution does not lie in neglecting the entity of governance but in developing valid avenues that allow low-risk experimentation. SMEs must create a simple AI use-case registry, a speedy review route or path over shared tools, a data sensitivity checklist, and a regulation mandating some human consideration when making decisions that impact the customers, employees, credit, safety or rights of the law. Such mechanisms lower the motivation of using hidden-tools and do not lower the visibility of organizations. They are also proponents of responsible human-AI cooperation. Previous studies of an automation-augmentation paradox caution that human judgment can hardly be substituted by AI in an uncontaminated manner; rather, human and machine tasks evolve as the users learn, trust, or excessively trust systems (Raisch and Krakowski, 2021). A related focus of human-centered AI research is on reliable, safe, and trustworthy systems with retention of meaningful human control (Jarrahi, 2018; Shneiderman, 2020).

➤ *Resilience Depends on Learning Loops, Not Paperwork Volume*

This result of highest resilience was attained when each of the two governance maturity and incident learning reinforced the others. This is in contact with the resilience literature, which regards resiliency as an ability that is built upon anticipation, coping, adapting, and learning against a state (Bhamra et al., 2011; Ducheck, 2020; Linnenluecke, 2017). Incident learning only enhanced resilience in the model when the organization updated controls, trained employees and enhanced the escalation routines in the aftermath of a disruption. When incidents merely generated blame or additional paperwork, resilience gains were feeble. The implication here is a warning to SMEs, therefore documentation does not have value unless it can be used to enhance future action. The risk register that has not been looked into, the AI policy that has not been properly grasped by the employees or the vendor checklist that has not made a difference in procurement decision does not do much to instill resiliency.

The contribution of slack resources is to be mentioned as well. With very limited time and budget at their disposal, AI governance seems to be a zero-sum matter to SMEs: each hour of compliance is another hour without customers, sales, or product development. The simulation demonstrates that a slight allocation of slack can alter this trend. An AI literacy recurrent budget, governance review, and incident learning can be incorporated into the budget at a modest annual cost, to enable the organization to establish routines, in the event of a significant failure. The discovery is in addition to SME adoption research that reveals that capabilities, resources, digital preparedness, and management assistance determine the success of AI adoption (Badghish and Soomro, 2024; Drydakis, 2022; OECD, 2025). It also endorses policy reports that cite that smaller firms have greater relative disadvantages

to AI adoption due to their lack of expert and absorptive capacity (G7 Italy, 2024).

➤ *Implications for Managers and Policymakers*

To the managers, the general consequence is obvious: AI governance should not be viewed as a policy paper that should be signed once. Creating a mini-AI decision system. The primary one must be an AI inventory where the tools, use cases, the owners, types of data, vendors, and risk tiers are registered. The second constituent must be a progressive vetting system, with low-risk internal productivity tools being superficially examined and decision-making of high impact being more seriously evaluated. Thirdly is an incident learning routine that should translate failures, near misses, inaccurate outputs, bias issues, privacy issues, and customer complaints into revised controls. The fourth element is an employee-training regime enhancing AI awareness. The practices do not entail enterprise level bureaucracy and the practices demand discipline.

To policymakers and standard setters, the findings imply that the proportionality and reusability should be prioritized in SME AI governance support. With regulatory expectations being converted into long documents only, numerous SMEs will either postpone the adoption of useful AI or neglect governance to the point of an incident happening. It should be supported with industry-specific templates, model AI libraries, third-party queries, no-harm use-cases, data sensitivity policies, and quick self-assessments. This will align with the risk-based focus of the EU AI Act and with the international management-systems, but would shortcut the gap between implementation in SMEs (European Parliament & Council, 2024; ISO/IEC, 2023a; NIST, 2023).

➤ *Theoretical Contribution*

The study contributes to three research streams. First, it contributes to AI governance research by showing that governance effectiveness depends on feedback timing, not only on the existence of controls. Second, it contributes to SME AI adoption research by explaining why the same governance mechanism can either suppress or enable innovation depending on maturity, delay, and reuse. Third, it contributes to organizational resilience research by identifying AI risk governance as a resilience-building capability. In this view, resilience is not separate from innovation. It is produced when innovation routines include risk sensing, monitoring, escalation, and learning. The model therefore bridges a gap between adoption studies that emphasize AI benefits and compliance studies that emphasize AI risks.

The system dynamics contribution is also methodological. Traditional cross-sectional studies are useful for estimating associations among adoption readiness, governance maturity, and performance. They are less able to represent accumulations, thresholds, and delayed side effects. The current model shows how a policy that looks efficient in month 6 may become risky by month 24, and how a policy that appears burdensome in the first year may become enabling once templates, skills, and trust accumulate. This

temporal explanation is essential for AI governance because AI tools, regulations, vendor platforms, and employee practices change quickly. A feedback model gives researchers and managers a way to test policy logic before costly implementation.

➤ *Limitations and Future Research*

The main limitation is that the results are normalized simulation outputs rather than observed longitudinal field measurements. This is acceptable for a theory-building system dynamics paper, but future research should calibrate the model with primary survey data, interview evidence, incident records, and workshop validation. Future studies should also compare sectors because AI risk profiles differ across retail, manufacturing, professional services, finance, health, education, and platform-based SMEs. Data sensitivity, customer impact, regulatory exposure, and vendor dependence are likely to change the location of the governance tipping point. Another limitation is that the model treats SMEs as organizational units, while real firms contain multiple departments, informal power structures, and uneven AI literacy. Future work can extend the model by adding employee-level adoption dynamics, vendor switching costs, cybersecurity incidents, and regulatory enforcement shocks.

Despite these limitations, the findings offer a practical and theoretically grounded message. SMEs should not copy the heavy compliance structures of large corporations, but they also cannot rely on informal experimentation alone. The strongest long-term position is balanced adaptive governance: small enough to be usable, strong enough to create accountability, and dynamic enough to learn. In that form, AI risk governance shifts from a compliance burden to an organizational resilience capability.

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.] Drydak, 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.] Forrester, J. W. (1968). Industrial dynamics after the first decade. Management Science, 14(7), 398-415.
- [15.] G7 Italy. (2024). Driving factors and challenges of AI adoption and diffusion in MSMEs. G7 Industry, Tech and Digital Ministerial Meeting.
- [16.] International Organization for Standardization. (2017). ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes. ISO.
- [17.] International Organization for Standardization/International Electrotechnical Commission. (2023a). ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system. ISO.
- [18.] International Organization for Standardization/International Electrotechnical Commission. (2023b). ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management. ISO.
- [19.] Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. Business Horizons, 61(4), 577-586. <https://doi.org/10.1016/j.bushor.2018.03.007>
- [20.] 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>
- [21.] 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>
- [22.] 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>
- [23.] Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management*, 58(3), 103434. <https://doi.org/10.1016/j.im.2021.103434>
- [24.] Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, 501-507. <https://doi.org/10.1038/s42256-019-0114-4>
- [25.] 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>
- [26.] 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>
- [27.] 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>
- [28.] OECD. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD.
- [29.] OECD. (2025). AI adoption by small and medium-sized enterprises. OECD Publishing.
- [30.] 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>
- [31.] 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>
- [32.] Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- [33.] Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe and trustworthy. *International Journal of Human-Computer Interaction*, 36(6), 495-504. <https://doi.org/10.1080/10447318.2020.1741118>
- [34.] Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. Irwin/McGraw-Hill.
- [35.] Sterman, J. D. (2002). *System dynamics: Systems thinking and modeling for a complex world*. Massachusetts Institute of Technology.
- [36.] 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>
- [37.] 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)
- [38.] Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
- [39.] 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>
- [40.] 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>