

Integrating Artificial Intelligence Governance into Business Excellence: A Design-Oriented Capability Framework for Small and Medium-Sized Enterprises in Emerging Europe

Prof. Zibeyda Shakaraliyeva*

UNEC, Baku, Azerbaijan

**Corresponding author, e-mail: shakaraliyeva_zibeyda@unec.edu.az*

Abstract. *Organizations that pursue business excellence increasingly rely on data-intensive and automated decision support. At the same time, managers face widening expectations regarding accountability, transparency, and societal impact when deploying artificial intelligence (AI). This paper develops a compact, design-oriented capability framework that helps small and medium-sized enterprises (SMEs) integrate AI governance into the continuous improvement routines of established excellence models. Building on an integrative synthesis of business excellence, Quality 4.0, and AI governance standards and policy guidance, the study translates high-level principles into auditable management practices that are feasible under resource constraints and high vendor dependence. The framework specifies six governance capabilities: (1) leadership accountability, (2) risk and impact assessment, (3) lifecycle controls for data and models, (4) transparent documentation, (5) human oversight and skills, and (6) ecosystem and supplier management. These capabilities are mapped to excellence dimensions and operationalized through a maturity rubric and decision templates that support readiness assessment and investment prioritization. The contribution is the integration logic: rather than proposing new AI governance principles, the paper shows how SMEs can embed existing governance requirements into excellence-based planning, audit, and corrective-action cycles while making trade-offs explicit for emerging European ecosystem contexts.*

Keywords: *artificial intelligence governance; business excellence; Quality 4.0; small and medium-sized enterprises; risk management; organizational capabilities; digital ecosystems.*

Introduction

The integration of artificial intelligence into everyday managerial decision-making has accelerated over the last decade. Forecasting, pricing, customer service, fraud detection, quality control, and internal assurance increasingly rely on predictive and generative techniques that learn from data rather than execute fixed rules. This shift creates a dilemma for organizations that pursue business excellence: the same technologies that enable productivity and innovation can also amplify operational risk, compliance exposure, and reputational damage when deployed without adequate governance.

Business excellence models help organizations balance performance and transformation by providing a structured logic for leadership, strategy deployment, process management,

learning, and results review (EFQM, 2020; NIST, 2023a). In an AI context, however, many firms experience a translation gap between these models and the socio-technical properties of algorithmic systems. AI-enabled processes can be non-deterministic, degrade through data and concept drift, and fail in ways that are difficult to detect until impacts materialize. Moreover, digital ecosystems mean that key components are frequently supplied by external vendors, reducing transparency and complicating accountability.

Large enterprises are increasingly institutionalizing responsible AI programs, but SMEs often lack the specialist functions and budgets required for enterprise-grade governance. Nevertheless, SMEs are exposed as deployers and suppliers in value chains that depend on algorithmic decision-making. Clients, regulators, and assurance providers increasingly expect evidence that SMEs can control data quality, monitor system performance, manage third-party dependencies, and provide meaningful human oversight. If AI governance is implemented as a standalone compliance add-on, it risks becoming brittle and underused; if it is integrated into management systems already used for quality and performance, it can become an enabling capability.

This paper addresses the following research question: How can SMEs integrate AI governance into business excellence systems in a way that improves reliability and accountability while remaining feasible under resource constraints and ecosystem dependence? The paper is positioned as a design-oriented conceptual contribution. It does not claim to discover new governance principles, nor does it empirically test performance effects. Instead, it synthesizes established excellence logics and AI governance requirements into a concise capability model with practical operationalization tools suitable for SMEs in emerging European markets.

The remainder of the paper is structured as follows. The literature review contrasts business excellence models with AI governance frameworks and identifies where integration is required. The methodology section explains the development process for the framework and its boundary conditions. The results present the six capabilities, an integration mechanism aligned to improvement cycles, and a maturity rubric for operationalization. The discussion outlines managerial implications and research propositions, and the paper concludes with limitations and directions for future validation.

Literature review

Business excellence models under digital and ecosystem conditions

Business excellence models translate organizational performance into assessable dimensions and improvement routines that align purpose and strategy with process execution and measurable results. The EFQM model frames excellence as an integrated approach to managing change and improving performance with attention to stakeholder value and transformation (EFQM, 2020). In the Baldrige tradition, excellence is operationalized through categories covering leadership, strategy, customers, measurement and knowledge management, workforce, operations, and results (NIST, 2023a). While models differ in terminology, they share a core logic: excellence emerges from coherent management systems rather than isolated initiatives.

Digital ecosystems intensify the relevance of excellence models because value creation increasingly spans organizational boundaries. Organizations depend on platform providers, cloud infrastructures, data brokers, and specialized software vendors. Ecosystem research argues that value capture depends on a firm's ability to coordinate interdependencies and align standards and incentives across complementors (Adner, 2017). For SMEs, ecosystem participation can provide access to advanced capabilities, including AI, but it also creates dependencies on third-party practices and opaque decision mechanisms.

A capability perspective helps explain why some organizations create durable value from digital technologies while others do not. The resource-based view links sustained advantage to valuable, rare, inimitable, and non-substitutable resources (Barney, 1991). Dynamic capability theory extends this logic by emphasizing the ability to sense opportunities, seize them through investment and business model choices, and transform routines over time (Teece, 2007). In ecosystem contexts, these theories imply that AI adoption is insufficient; firms must develop governance and learning routines that maintain performance under uncertainty and shared accountability.

From Quality 4.0 to algorithmic excellence

Quality management scholarship increasingly recognizes that digital technologies reshape excellence systems. The concept of Quality 4.0 positions analytics, automation, and digital tools as enablers of quality and excellence while emphasizing that governance and workforce capabilities must evolve alongside technology (Fonseca, 2021). When predictive or generative models are embedded in operational processes, quality outcomes depend on data provenance, model performance, and the appropriateness of human oversight - elements not always explicit in traditional process maps.

Algorithmic systems create specific challenges for excellence routines. Internal audits, management reviews, and corrective actions remain relevant, but the control object changes: organizations must manage lifecycle risks (data drift, model updates, emergent behavior) and socio-technical impacts (automation bias, fairness concerns, interpretability limits). Consequently, organizations require a translation layer that connects excellence routines to AI-specific governance mechanisms in a way that is auditable and resource-proportionate.

AI governance frameworks: overlap and integration gaps

AI governance can be defined as the set of structures, processes, and controls through which an organization directs and oversees the development and use of AI to achieve objectives while managing risks and impacts. ISO/IEC 42001 specifies requirements for establishing and continually improving an AI management system, emphasizing accountability, risk treatment, documentation, and improvement (ISO, 2023). The NIST Artificial Intelligence Risk Management Framework provides a voluntary, lifecycle-based approach organized around governance, context mapping, measurement, and risk response (NIST, 2023b). At the level of principles, the OECD recommendation emphasizes human-centered values, transparency, robustness, and accountability (OECD, 2019).

This paper does not dispute that these frameworks already cover many required governance elements. The integration gap lies elsewhere: (1) excellence models provide the managerial improvement logic but are relatively silent on algorithmic lifecycle controls; (2) AI governance frameworks specify controls but are not inherently embedded in the day-to-day routines that excellence systems use for planning, auditing, and corrective action; and (3) SMEs face feasibility constraints that require proportionality, templating, and reuse of existing governance infrastructure.

Generative systems amplify governance requirements because outputs may be difficult to predict and can include hallucinations, copyright issues, or leakage of sensitive information. Research on large language models highlights that responsible deployment requires transparency and careful risk management (Bender, Gebru, McMillan-Major, & Shmitchell, 2021). For SMEs, a recurring governance risk is informal adoption: employees may use general-purpose tools without formal procurement, reducing control over data protection and oversight.

Contextualization: SMEs in emerging European markets

The emerging Europe context matters because many SMEs operate in cross-border value chains where customers, insurers, and regulators increasingly require evidence of governance maturity. At the same time, SMEs commonly rely on external vendors for AI capabilities, face limited internal legal and risk expertise, and operate under resource constraints that make heavy governance bureaucracy impractical.

Accordingly, an integration framework for this context should satisfy three design requirements: (i) it must be compatible with excellence routines already used for quality and performance; (ii) it must be auditable using lightweight artifacts and clear ownership; and (iii) it must explicitly cover ecosystem dependencies and supplier controls, because vendor behavior can materially shape risk exposure.

Methodology

The study follows a design-oriented development process grounded in integrative synthesis. The goal is to produce a coherent capability framework and operationalization tools that are consistent with established bodies of knowledge and usable in practice, rather than to test causal relationships or generalize statistically.

Stage 1: Integrative synthesis. The source corpus combined (a) business excellence and quality management literature (EFQM, Baldrige, Quality 4.0), (b) organizational capability perspectives (RBV and dynamic capabilities), and (c) AI governance standards, policy instruments, and risk management guidance (e.g., ISO/IEC 42001, NIST AI RMF, OECD principles, EU AI Act). A structured search was conducted using combinations of keywords such as 'business excellence', 'EFQM', 'Baldrige', 'Quality 4.0', 'AI governance', 'responsible AI', 'AI risk management', 'model lifecycle', 'third-party risk', and 'SME'. Backward and forward citation searches were used to identify influential work and to triangulate academic and practitioner sources.

Stage 2: Capability extraction and consolidation. Control requirements and mechanisms were coded into an initial long list. Similar items were merged and organized around recurring governance functions (accountability, risk assessment, lifecycle control, documentation, human oversight, and ecosystem management). Alternative decompositions were considered (e.g., separating data governance from model governance, or splitting transparency into internal documentation and external disclosure). The final set was selected to minimize overlap while preserving coverage of the control universe demanded by standards and assurance practice.

Stage 3: Excellence mapping and operationalization. The consolidated capabilities were mapped to common excellence dimensions (leadership, strategy, processes, knowledge, workforce, partnerships) and embedded into the plan-do-check-act logic used in many excellence systems. To support implementation, the paper develops a maturity rubric and lightweight templates (system cards, risk-impact assessment, supplier due diligence checklist) that translate capabilities into auditable routines. The framework is therefore best interpreted as a design artifact: internally consistent, grounded in authoritative guidance, and intended to be evaluated and refined through future empirical work.

Results and discussion

Six AI governance capabilities for SMEs

The synthesis converged on six governance capabilities that jointly cover the minimum management system required to create reliable value from AI in SMEs. The capabilities are not presented as the only possible decomposition; rather, they represent a compact structure that aligns with both excellence models and dominant AI governance frameworks while remaining implementable in resource-constrained settings.

1) Leadership accountability. Leadership accountability requires explicit ownership for each AI use case, clear decision rights for deployment and retirement, and escalation paths for incidents and unacceptable impacts. In SMEs, a practical mechanism is to extend existing governance bodies (e.g., quality councils, risk committees) with an AI governance agenda and to assign a named owner for each system card.

Design tension: centralized accountability vs. local autonomy for business units

Design tension: speed of deployment vs. quality gate rigor

2) Risk and impact assessment. Risk and impact assessment covers intended use, affected stakeholders, plausible failure modes, and the severity and likelihood of harms, along with documented mitigations and residual risk acceptance. For SMEs, proportionality is critical: low-impact use cases can rely on simplified checklists, while higher-impact cases require stronger validation evidence, controls, and human oversight.

Design tension: proportionality vs. completeness of assessment

Design tension: standardization of templates vs. context-specific judgment

3) Lifecycle controls for data and models. Lifecycle controls include data sourcing rules, access controls, validation of training and operational data, monitoring for drift, and criteria for retraining and rollback. For generative use cases, lifecycle control also includes prompt

management, retrieval resources, and usage policies. A feasible SME mechanism is to define a small set of monitoring indicators (e.g., error rates, override frequency, incident recurrence) and integrate them into existing performance dashboards.

Design tension: monitoring depth vs. operational cost

Design tension: stability of models vs. rapid iteration and experimentation

4) Transparent documentation. Transparent documentation is a coordination mechanism: it makes assumptions, limitations, and responsibilities explicit and supports auditability and continuity when staff turnover occurs. Documentation should be concise to remain sustainable in SMEs. A practical pattern is a short system card for each use case capturing purpose, data sources, decision logic, performance metrics, key risks, mitigations, owners, and a change log.

Design tension: documentation sufficiency vs. administrative burden

Design tension: internal transparency vs. disclosure constraints with vendors

5) Human oversight and skills. Human oversight requires defining when human review is mandatory, training users to detect errors, and ensuring escalation procedures are realistic. Governance should explicitly address automation bias and clarify accountability when humans rely on AI outputs. SMEs can extend existing competence frameworks with role-specific AI competencies (data classification, prompt hygiene, interpretation of outputs, and incident reporting).

Design tension: human-in-the-loop control vs. efficiency gains from automation

Design tension: specialist expertise vs. broad baseline literacy across staff

6) Ecosystem and supplier management. Ecosystem and supplier management addresses the fact that SMEs rarely build AI end-to-end and therefore inherit risk through vendor dependencies. Governance mechanisms include supplier due diligence, contractual clauses for transparency and incident reporting, model update notification, data processing terms, and verification of third-party controls. Procurement and quality functions can jointly define a minimum supplier control set aligned to enterprise customer expectations.

Design tension: vendor opacity vs. assurance needs

Design tension: standardized supplier controls vs. negotiation leverage of SMEs

Embedding capabilities into an excellence improvement cycle

The integration mechanism is to embed the six capabilities into the routines SMEs already use for business excellence rather than creating a parallel governance bureaucracy. Many SMEs use variants of the plan-do-check-act cycle through quality management systems or internal audit programs. In an AI context, planning includes defining use cases and expected value, performing proportional risk and impact assessment, and establishing ownership and documentation. Doing includes implementation and change management, supplier onboarding, and the establishment of lifecycle monitoring. Checking includes performance measurement, incident review, and internal audits that test whether controls operate as designed. Acting includes corrective actions, retraining decisions, policy updates, and workforce development.

This logic is consistent with Baldrige process maturity concepts, which assess approach, deployment, learning, and integration alongside results levels and trends (NIST, 2023a). Applied

to AI governance, maturity questions include whether risk assessments are systematic, whether controls cover all relevant use cases (including shadow use), whether incident learnings update procedures, and whether governance is integrated with strategy, budgeting, and supplier management.

Operationalization: maturity rubric and auditable artifacts

To make the framework usable for readiness assessment, Table 2 provides a lightweight maturity rubric for each capability. The rubric avoids false precision by using observable artifacts and routines rather than purely numerical scores. It can be used for self-assessment, internal audit scoping, or supplier discussions.

Table 1. Mapping business excellence dimensions to AI governance capabilities

Business excellence dimension	Governance capability	Operational mechanism in SMEs
Leadership and purpose	Leadership accountability	Assign use case owners; define decision rights; incident escalation paths
Strategy and stakeholders	Risk and impact assessment	Proportional assessments integrated into approvals and change management
Process management	Lifecycle controls for data and models	Data validation; monitoring; drift detection; retraining and rollback criteria
Knowledge management	Transparent documentation	System cards; validation evidence; change logs; audit trail for decisions
Workforce and learning	Human oversight and skills	User training; review triggers; procedures to mitigate automation bias
Partnerships and value chains	Ecosystem and supplier management	Supplier due diligence; contract clauses; verification of third-party controls

Source: Author's own synthesis.

Table 1 provides the integration bridge: SMEs can leverage existing excellence routines (management reviews, internal audits, process documentation) to operationalize AI governance without duplicating governance structures. This mapping is not intended as a one-to-one equivalence between models; rather, it functions as a practical translation layer that supports communication with internal and external stakeholders.

Table 2. Maturity rubric for AI governance capabilities in SMEs

Capability	Foundational (minimum viable)	Managed (repeatable and auditable)	Adaptive (learning and improvement)
Leadership accountability	Named owner per use case; basic escalation path.	Decision rights documented; governance agenda in leadership reviews; incident roles defined.	Governance updated based on incidents and strategy; ownership persists through lifecycle changes.
Risk and impact assessment	Checklist for intended use, stakeholders, and basic risks.	Risk level linked to required controls; mitigations documented; approvals recorded.	Assessments updated after incidents and changes; portfolio view of risk across use cases.
Lifecycle controls for data and models	Data sources listed; access controls; baseline performance check.	Monitoring indicators defined; drift checks; retraining/rollback criteria; change control.	Continuous monitoring with thresholds; post-change validation; learning loop from performance deviations.
Transparent documentation	System card with purpose, data sources, owner, and limitations.	Versioned documentation; change log; validation evidence stored and retrievable.	Documentation informs design improvements; supports audits and supplier negotiations.

Human oversight and skills	Users trained on safe use; clear review triggers for high-impact decisions.	Role-based training; documented override and escalation; periodic competence refresh.	Feedback and incident data used to improve guidance; oversight calibrated to observed failure modes.
Ecosystem and supplier management	Supplier due diligence checklist; basic data processing terms.	Contract clauses for updates and incidents; service metrics; periodic vendor review.	Multi-supplier contingency planning; joint improvement with vendors; alignment with customer assurance needs.

Source: Author's own synthesis.

Implications and research propositions

From a managerial perspective, the framework supports sequencing under resource constraints. SMEs can start with leadership accountability and documentation (to establish ownership and auditability), then implement proportional risk assessment and supplier controls, and finally strengthen lifecycle monitoring and workforce training as AI use scales.

From a research perspective, the framework yields testable propositions that should be evaluated empirically rather than treated as demonstrated results. First, higher maturity in the six capabilities should be associated with fewer governance incidents (e.g., data leakage, unacceptable outputs) and higher perceived reliability of AI-enabled processes. Second, integration of AI governance into excellence routines should reduce the cost of compliance compared to standalone governance efforts, by reusing management reviews and audit cycles. Third, ecosystem position and customer assurance pressure are likely to moderate governance choices, with supplier management becoming more salient as vendor dependence increases.

Conclusion

This paper developed a design-oriented capability framework that integrates AI governance into business excellence systems for SMEs in emerging European markets. Building on excellence model logic and authoritative AI governance standards and policy guidance, the framework identifies six capabilities and provides an integration mechanism that embeds them into continuous improvement routines.

The contribution is primarily integrative and operational: it packages existing governance requirements into an excellence-compatible structure and offers a maturity rubric and lightweight artifacts that support readiness assessment and investment prioritization. The paper does not claim empirical validation of performance effects. Future work should develop measurement

scales for each capability, pilot the rubric in SMEs, and study how governance maturity relates to operational resilience, innovation outcomes, and customer trust in ecosystem settings.

Limitations include the conceptual nature of the contribution and the absence of longitudinal or comparative empirical data. However, the framework provides a structured basis for subsequent qualitative case studies, surveys, and maturity assessments that can test and refine the proposed capability set and its assumed trade-offs.

References

- Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of Management*, 43(1), 39-58. <https://doi.org/10.1177/0149206316678451>
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99-120. <https://doi.org/10.1177/014920639101700108>
- Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610-623). Association for Computing Machinery. <https://doi.org/10.1145/3442188.3445922>
- EFQM. (2020). The EFQM model. European Foundation for Quality Management.
- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.
- Fonseca, L. M. (2021). Quality 4.0: The EFQM 2020 model and Industry 4.0 relationships and implications. *Sustainability*, 13(6), 3107. <https://doi.org/10.3390/su13063107>
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337-355.
- ISO. (2023). ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system. International Organization for Standardization.
- NIST. (2023a). 2023-2024 Baldrige Excellence Builder. National Institute of Standards and Technology.
- NIST. (2023b). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-1>
- OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Organisation for Economic Co-operation and Development.
- 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>
- Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356-367. <https://doi.org/10.1177/1534484305278283>