From Frameworks to Feasible Practice: A Modular AI Governance Blueprint for Consulting SMEs

DOI: 10.12776/qip.v30i1.2336

Ludmila Jiříčková, Petr Doucek

Received: 01-03-2026 Accepted: 13-04-2026 Published: 30-04-2026

ABSTRACT

Purpose: To address the growing gap between Artificial Intelligence (AI) governance expectations and the practical capacities of consulting small and medium enterprises (SMEs).

Methodology/Approach: Conceptual review and comparative analysis of leading governance regimes and standards, followed by mapping to enterprise risk management models commonly used to manage organisational risks.

Findings: The paper shows that consulting SMEs face compounded barriers (limited compliance capacity, data constraints, cultural resistance, algorithm aversion, and regulatory uncertainty) that make comprehensive governance unrealistic. It derives a modular governance blueprint that supports gradual implementation aligned with quality management and risk appetite.

Research Limitation/Implication: The blueprint requires operationalisation into checklists, templates, and measurable indicators and should be validated across multiple SME cases and AI use scenarios.

Originality/Value of paper: The key contribution is translating heterogeneous AI governance sources into a feasibility-first governance logic for SMEs, framed as a quality and trust enabler rather than a compliance-only burden.

Category: Conceptual paper

Keywords: AI risk and opportunities; management of consulting SMEs; enterprise risk frameworks; adaptive governance models; regulatory compliance innovation

Research Areas: Management of Technology and Innovation; Quality by Innovation

1 INTRODUCTION

Artificial Intelligence (AI) has transitioned from a futuristic concept to an integral element of organisational strategy and operations. This transformation brings unprecedented opportunities, but also novel risks and governance challenges. AI governance can be defined as the framework of policies, processes, and structures that ensure the ethical, safe, and accountable use of AI within organisations (Radu, 2021; Papagiannidis, Mikalef, & Conboy, 2025).

In recent years, a proliferation of AI governance frameworks has emerged at international and national levels – from high-level principles to regulatory acts and technical standards – aiming to guide the responsible development and deployment of AI. Simultaneously, risk management models are being applied and adapted to address the unique uncertainties introduced by AI technologies (Schiff et al., 2021).

Such adaptation is consistent with risk management scholarship emphasising that advances should remain grounded in risk assessment foundations and explicit treatment of uncertainty (Aven, 2016). This principles-to-practice gap is widely discussed for small and medium enterprises (SMEs) and is particularly salient in knowledge-intensive sectors such as consulting. Consulting SMEs thrive on human expertise, trust-based client relationships, and agile cultures, which create challenges for adopting and implementing AI tools. They often lack the resources and formal structures of large firms to implement comprehensive governance, while any misstep can erode client trust, a core asset in professional services (Armour & Sako, 2020). This article provides a theoretical overview of AI governance and AI-related risk management with a focus on the consulting SME context. The first part provides an overview of major AI governance frameworks: Organisation for Economic Co-operation and Development (OECD) principles, European Union (EU) AI Act, International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) 42001:2023, National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) and their scope, principles, and implementation challenges. The following section reviews selected risk typologies and organisational risk management models relevant to AI: ISO 31000:2018, Committee of Sponsoring Organisations of the Treadway Commission Enterprise Risk Management (COSO ERM), and the Three Lines of Defence model and their contribution to AI risk management. Finally, the paper critically assesses consulting SME requirements for AI governance.

Beyond review and comparison, the paper proposes a modular AI governance blueprint for consulting SMEs. The blueprint is designed as a minimum viable governance set that can be expanded over time and mapped to external requirements (regulations and standards) and internal risk governance structures. This shifts the discussion from what responsible governance should look like in principle to what can be implemented credibly in resource-constrained professional services.

2 METHODOLOGY

This article is conceived as a theoretical overview and critical assessment of the issue of artificial intelligence governance with a specific focus on the context of small and medium-sized enterprises in the consulting sector. The methodological procedure used in this study is qualitative and interpretative, focusing on the synthesis of existing theoretical frameworks, regulatory acts, and management standards, with the goal of identifying their applicability in the practice of SMEs. The analytical approach was divided into three main phases: selection and analysis of key governance frameworks, comparative assessment of risk management models, and contextualization for the specifics of consulting SMEs.

3 EVOLUTION OF AI GOVERNANCE FRAMEWORKS

The governance of AI has evolved through a combination of soft law principles, hard law regulations, and standards developed by international bodies and governments in response to the fast-paced adoption of AI and its societal impacts (Jobin, Ienca, & Vayena, 2019; Batool, Zowghi, & Bano, 2025). This section reviews four cornerstone frameworks: the OECD AI Principles, the European Union's AI Act, the ISO/IEC 42001:2023 AI management system standard, and the NIST AI Risk Management Framework. Each reflects a different level of governance – from broad values, to binding regulation, to implementation guidance – and each entails distinct principles and challenges for implementation.

3.1 OECD AI principles

One of the first global attempts to articulate AI governance principles was led by the Organisation for Economic Co-operation and Development (OECD). In May 2019, the OECD adopted a set of AI Principles, representing the first internal standard for AI governance. These principles, endorsed by OECD members and G20 countries, were updated in 2024 to account for recent technological developments (OECD, 2024). The OECD AI Principles set out a vision for trustworthy AI. It is human-centric and aligned with democratic values. The OECD AI Principles define five value-based pillars for trustworthy AI: inclusive growth and well-being; human-centred values and fairness; transparency and explainability; robustness, security and safety; and accountability (OECD, 2024; Floridi et al., 2018).

Complementary to the principles, the OECD recommendation also calls on governments to enable trustworthy AI through investment, ecosystem-building, capacity development, agile regulation and international co-operation (OECD, 2024). The OECD AI Principles helped establish a shared vocabulary and baseline for responsible AI across jurisdictions (Radu, 2021; Jobin, Ienca, & Vayena, 2019). However, as value-based guidance, they remain non-prescriptive: their impact depends on voluntary adoption and translation into concrete organisational practices (Schiff et al., 2021).

3.2 EU AI Act

The European Union's Artificial Intelligence Act (adopted as Regulation (EU) 2024/1689) introduces a risk-based approach that classifies AI systems by risk and applies proportionate obligations, with the most extensive requirements reserved for high-risk AI (European Commission, 2021; Veale & Zuiderveen Borgesius, 2021). In brief, the Act distinguishes prohibited uses (unacceptable risk), high-risk systems subject to strict controls, limited-risk systems with transparency duties, and minimal-risk uses with few or no obligations.

For prohibited AI, the Act bans practices such as social scoring by governments and real-time biometric identification in public (with narrow exceptions) as these uses are deemed to undermine core rights (Veale & Zuiderveen Borgesius, 2021). The high-risk category includes AI in critical areas such as medical devices, hiring, credit scoring, education, transport, and law enforcement, etc. Providers of high-risk AI systems must comply with rigorous requirements before and after market deployment, including conformity assessments. Key obligations are ensuring high-quality training data (to minimise bias), technical documentation and logging for traceability, transparency to users, human oversight, robustness and cybersecurity measures, among others (European Commission, 2021). These requirements align with principles of accountability and transparency by mandating that AI systems be auditable and under meaningful human control when they significantly impact people (Floridi et al., 2018).

Substantively, the EU AI Act shifts AI governance from voluntary ethics to binding legal compliance and operationalises abstract principles into enforceable requirements for high-risk systems (e.g. documentation, human oversight and risk management) (European Commission, 2021; Floridi et al., 2018). This raises questions about definitional clarity, enforcement capacity and the balance between risk mitigation and innovation, which are particularly challenging for SMEs with limited compliance resources (Veale & Zuiderveen Borgesius, 2021).

The EU AI Act seeks balance through a field approach and by exempting low-risk innovation sandboxes. The real impact will depend on implementation details and forthcoming harmonised standards. For organisations, the AI Act effectively makes AI risk management and governance mandatory, not optional. Firms deploying AI in Europe will need internal compliance programs – including data governance, impact assessments for AI (similar to data protection impact assessments), record-keeping, and incident reporting – to meet the law's requirements (European Commission, 2021). For SMEs in particular, which often lack dedicated compliance staff, this could pose a formidable challenge, as discussed later in this article. In summary, the EU AI Act is a landmark regulatory framework translating AI governance principles into enforceable rules, though it raises questions about feasibility and support needed, especially for smaller actors, to comply (Veale & Zuiderveen Borgesius, 2021).

3.3 ISO/IEC 42001:2023 – AI management system standard

ISO/IEC 42001:2023 is the first international, certifiable AI management system standard, using a Plan-Do-Check-Act (PDCA) cycle to embed lifecycle governance and operationalise goals expressed in principles and regulation (ISO/IEC 42001, 2023; Batool, Zowghi, & Bano, 2025; Laux, Wachter, & Mittelstadt, 2024). While certification can signal assurance, consulting SMEs may benefit most from selectively adopting key controls rather than pursuing full-scale certification.

Under ISO/IEC 42001:2023, organisations implementing an Artificial Intelligence Management System (AIMS) are expected to establish policies and procedures covering the entire AI life cycle. The life cycle spans the development and acquisition of AI systems through deployment, monitoring, and decommissioning (ISO/IEC 42001, 2023). The standard emphasises key components of AI governance. Under ISO/IEC 42001:2023, organisations implement an AI Management System across the AI lifecycle by defining governance roles, integrating AI risk management (e.g. bias, safety, cybersecurity and legal compliance), embedding ethical principles, and establishing monitoring, continual improvement and stakeholder engagement processes (ISO/IEC 42001, 2023; Benraouane, 2024).

To conclude, ISO/IEC 42001:2023 is a milestone in translating AI governance principles into organisational practice. The key approach is through a management system that emphasises continuous risk management and oversight. The success of implementation will depend on providing modular and adaptive solutions.

3.4 NIST AI risk management framework (RMF) 1.0

Another major contribution to AI governance comes from the United States' National Institute of Standards and Technology (NIST), which released the AI Risk Management Framework (AI RMF) 1.0 in January 2023 (Tabassi, 2023). The NIST AI RMF is a voluntary framework intended to help organisations systematically identify, assess, and manage the risks of AI systems (Raji et al., 2020). It was developed through a multistakeholder process (industry, academia, government), building on NIST's experience with frameworks like the Cybersecurity Framework, and is envisaged as a de facto reference for AI governance best practices in the U.S. and internationally (Tabassi, 2023). The overarching aim of the NIST AI RMF is to improve the trustworthiness of AI by encouraging organisations to integrate considerations of safety, security, fairness, transparency, accountability, and privacy into the AI lifecycle (Tabassi, 2023; Floridi et al., 2018; Batool, Zowghi, & Bano, 2025).

The AI RMF is organised around four core functions that an organisation's AI risk management process should continuously perform: Govern, Map, Measure, and Manage. These are conceptually similar to phases of risk management but tailored to AI. By structuring AI risk management into these functions, the NIST

framework supports a continuous improvement loop for AI governance, rather than a one-time checklist (Tabassi, 2023). The literature has praised the AI RMF for offering a pragmatic and flexible approach that organisations can adapt to their needs (Batool et al., 2025; Radu, 2021). It does not mandate specific metrics or methods but provides a taxonomy and process that can integrate with existing risk management programs. Notably, NIST also released a companion AI RMF Playbook with suggested actions and an illustrative crosswalk mapping the AI RMF functions to other standards (like ISO/IEC 42001:2023 and the EU AI Act requirements) (Mehrabi et al., 2021; Schiff et al., 2021).

However, like any voluntary framework, its impact depends on organisational commitment. One critique is that smaller organisations might find it difficult to implement the full breadth of the framework due to resource constraints (Batool, Zowghi, & Bano, 2025). Another challenge is in the Measure function, where it can be difficult to develop meaningful metrics for complex properties such as "fairness" or "explainability". The literature points to a need for more standardised tools and benchmarks in this area (Mehrabi et al., 2021; Schiff et al., 2021).

4 AI RISK TYPOLOGIES AND RISK MANAGEMENT MODELS FOR AI

Risk management is a well-established discipline in organisational management, providing frameworks for identifying and addressing potential events that could negatively (or positively) affect objectives. The advantage of AI introduces new risk considerations that may not be fully addressed by traditional risk management approaches. In this section, typologies of AI-related risks are outlined as identified in current literature.

4.1 Typologies of AI-related risks

AI systems present a spectrum of risks that can be categorised in various ways. A consistent theme in the literature is classifying AI risks by their nature (technical vs. non-technical) or impact area. The literature commonly groups AI-related risks into four overlapping categories: technical risks (performance, robustness and security vulnerabilities), legal/compliance risks (data protection, IP, and regulatory obligations), ethical/social risks (privacy, transparency, discrimination, and broader societal impacts), and reputational/strategic risks (trust damage, misinvestment and over-reliance) (Batool, Zowghi, & Bano, 2025; Brundage et al., 2020).

These categories often overlap. For instance, a technical risk (bias) can manifest as an ethical risk (discrimination), which then becomes a reputational risk. The EU's risk-based approach effectively combines these considerations by focusing on the severity of impact on safety or rights (European Commission, 2021; Veale & Zuiderveen Borgesius, 2021). The literature encourages organisations to perform risk assessments specifically for AI systems. The purpose of risk

typologies is to ensure a comprehensive view: when deploying AI, one should ask – have we considered the technical reliability? The regulatory compliance? The ethical implications? The possible reputational fallout? By categorising, organisations can assign appropriate expertise to manage each (engineers for technical, compliance officers for legal, ethicists or diverse stakeholders for social, etc.).

For consulting SMEs, an additional struggle is opportunity risk – missing out on the benefits of AI (like improved efficiency or insight) can be a strategic risk in itself. Thus, many refer to "AI Risk and Opportunity Management" as a paired concept (Radu, 2021; Batool, Zowghi, & Bano, 2025). This is akin to ensuring that fear of risks does not lead to stagnation. Instead, risks are managed so that AI's opportunities (better data analysis, enhanced services, new business models) can be seized confidently. For instance, Armour & Sako (2020) observed that professional service firms face the challenge of integrating AI into their business models (like offering AI-driven continuous services). This is a competitive advantage; not doing this could mean falling behind competitors. Therefore, governance must balance the mitigation of the risks identified above with the facilitation of innovations.

4.2 Traditional risk management frameworks applied to AI

ISO 31000:2018 defines risk as the effect of uncertainty on objectives and provides a generic process (context → identify → analyse/evaluate → treat → monitor/communicate) that can be tailored to any organisation (ISO 31000, 2018). This ISO framing aligns with risk scholarship that treats risk assessment as an iterative process linking uncertainty, evidence and decision-making (Aven, 2016). For AI, it offers SMEs a disciplined way to log AI-related uncertainties, assess likelihood and impact, and select proportionate controls or monitoring. Its limitation is generality: it does not specify AI metrics, roles or tools, so SMEs must translate it into concrete responsibilities and practices.

Organisations can leverage existing risk management frameworks to govern AI-specific risks. Three widely cited approaches are ISO 31000:2018, COSO Enterprise Risk Management (ERM), and the Three Lines of Defence model. Each framework and model offers a perspective on risk governance that remains relevant in the AI era, although some adaptation may be needed.

COSO ERM embeds risk management into strategy and performance, emphasising leadership oversight and explicit risk appetite (COSO, 2017; Fraser & Simkins, 2016). Its five components—governance & culture; strategy & objective-setting; performance; review & revision; and information, communication & reporting—support organisation-wide risk-informed decision-making. For consulting SMEs, the main value is aligning AI adoption with strategic objectives and clarifying tolerable levels of error/bias in client work, but full COSO-style implementation can be resource-intensive and therefore requires simplification (COSO, 2017).

For AI, COSO's emphasis on governance is key. It aligns with calls to treat AI risks not just as technical issues but as board-level issues, given the potential impact on company reputation and strategy (e.g. if an AI product fails, it can be as damaging as a financial misstatement) (COSO, 2017). The COSO approach would advocate that consulting SMEs define their AI risk solution (how much risk of error or bias are we willing to tolerate in our services?), involve top leadership in major AI-related decisions, and integrate AI risk metrics into their overall performance dashboards. A notable insight from COSO is linking risk to value creation – it recognises that to achieve strategic goals, taking some risk is necessary, so the goal is to manage risk in pursuit of value, not eliminate it (COSO, 2017; Fraser & Simkins, 2016). In the AI context, this resonates with the idea of leveraging AI for competitive advantage while controlling downsides. One drawback is that COSO's full implementation can be resource-intensive and formal, expecting distinct risk officers, extensive documentation, etc. (COSO, 2017; Fraser & Simkins, 2016). SMEs might not have separate compliance departments or risk committees; often, the owner or partners collectively handle these roles. So applying COSO in a small firm means simplifying – e.g. assigning one partner to champion AI risk oversight, rather than a full risk office, but still ensuring that person reports at leadership meetings about AI risk issues.

The Three Lines of Defence (3LoD) model (recently updated to the "Three Lines Model" by the Institute of Internal Auditors, 2020) provides a clear delineation of risk management roles:

- First line – operational management (people who own and manage risks in their day-to-day operations),
- Second line – risk management and compliance functions (specialists who coordinate, monitor and facilitate effective risk management),
- Third line – internal audit (providing independent assurance) (IIA, 2020).

In consulting SMEs, the first line is the project team using AI and performing day-to-day controls and review of AI-assisted outputs; the second line (a designated risk/compliance lead) sets policies, coordinates training and monitors adherence; and the third line provides independent assurance, often via periodic internal or external review (IIA, 2020; Veber, Nedomová, & Doucek, 2016). Because SME roles often merge, proportionality can be achieved through lightweight separation of duties and external checks when needed (IIA, 2020).

Table 1 – Comparison of frameworks and models in relation to AI governance for SMEs (Source: Authors)

Framework	Strengths for AI Governance	SME Relevance
NIST AI RMF	Practical, flexible, risk-focused	Scalable and modular
ISO 31000:2018	Universally adaptable, process-based	Requires tailoring, good for starters
COSO ERM	Strategic alignment, risk appetite	Governance-heavy, can be simplified
3 LoD Model	Role clarity, oversight separation	Role may be merged in SMEs, but still valuable

Each of these frameworks has something to contribute to AI governance, as indicated in Table 1. A recent analysis concluded that no single framework alone suffices for managing AI risks in SME. ISO 31000:2018 offers flexibility and processes, COSO provides strategic integration, and 3LoD offers structural clarity. Together, they form a strong foundation for managing risks and opportunities of using AI tools in everyday practice for consulting SMEs.

5 AI GOVERNANCE CHALLENGES IN CONSULTING SMES

Small and medium-sized consulting firms could significantly profit from AI tools. For instance, automating data analysis, improving predictions, or enhancing knowledge management could boost their productivity and service quality. However, these firms also face distinct governance challenges when adopting AI, compared to large organisations, as shown in Table 2 below. In this section, the paper will focus on the specific hurdles consulting SMEs encounter. Limitations are in resources and expertise, issues of trust (both within the firm and with clients), and cultural or structural factors.

Table 2 – Comparison of frameworks for AI governance in relation to AI risk management and relevance for SMEs (Source: Authors)

Framework	Strengths for AI Risk Management	SME Relevance
OECD AI Principles (2024)	Value-based orientation; explicit emphasis on accountability, robustness, transparency and human oversight; strong normative foundation for identifying ethical and societal AI risks	High-level and non-operational; suitable as a *conceptual compass* but insufficient on its own for risk implementation in SMEs
EU AI Act	Legally binding, risk-based categorisation of AI systems; explicit obligations for high-risk AI (risk management, human oversight, documentation, monitoring); strong enforcement mechanisms	High compliance burden; challenging for SMEs without legal and compliance capacity; requires simplification and external support to be feasible
ISO/IEC 42001:2023	Management-system approach to AI risks; lifecycle-based risk identification, treatment and monitoring; PDCA cycle supports continuous improvement	Scalable in principle but resource-intensive; SMEs benefit from selective or partial adoption rather than full certification
NIST AI RMF 1.0	Explicitly risk-focused; structured around Govern–Map–Measure–Manage; integrates technical and organisational risk perspectives; flexible and non-prescriptive	Highly suitable for SMEs due to modularity and adaptability; supports incremental implementation aligned with existing practices

5.1 Key barriers to AI governance implementation in SMEs

Literature and industry surveys identify a “vicious circle” of barriers that SMEs often face in adopting and governing AI (Batool, Zowghi, & Bano, 2025; Sánchez, Calderón, & Herrera, 2025). Recent evidence from IT risk management practice during Covid-19 illustrates how quickly risk processes must adapt to external

shocks, reinforcing the need for lightweight, adaptive governance (Maryška, Nedomová, & Doucek, 2020). These barriers tend to reinforce one another, making it challenging for smaller firms to break into effective AI utilisation.

The prominent obstacles include:

- Limited Resources and Expertise: SMEs often lack financial and specialised human resources for AI adoption, limiting their ability to implement governance best practices and increasing reliance on vendors (Sánchez, Calderón, & Herrera, 2025; Batool, Zowghi, & Bano, 2025). Fragmented data and infrastructure further reduce data quality and raise error risk (OECD, 2024; Yang, Blount, & Amrollahi, 2024);
- Trust Issues and Algorithm Aversion: Skepticism and algorithm aversion can lead to underuse of AI tools, duplicative work and reduced efficiency (Dietvorst, Simmons, & Massey, 2015; Logg, Minson, & Moore, 2019). In consulting contexts, reputational concerns and fear of role displacement can further increase caution (Armour & Sako, 2020; Yang, Blount, & Amrollahi, 2024);
- Organisational Culture and Change Resistance: Cultures built on human expertise and personalised service may resist standardisation or automation through AI, while leadership's low tolerance for failure limits experimentation (Schein, 2017; Armour & Sako, 2020). This often results in delayed adoption or minimal pilots (Batool, Zowghi, & Bano, 2025);
- Data and Technological Constraints: Limited data readiness (unstructured, inconsistent or poorly governed data) and legacy IT constraints reduce feasibility (OECD, 2024; Yang, Blount, & Amrollahi, 2024). From a business informatics perspective, the 'enterprise architect' role can help align data, processes and Information and Communication Technologies (ICT) governance, reducing fragmentation that undermines AI governance (Helfert, Doucek, & Maryška, 2013). Necessary upgrades and cybersecurity controls can be costly to justify without immediate returns (European Commission, 2021; Veale & Zuiderveen Borgesius, 2021);
- Regulatory Uncertainty and Limited External Support: Rapidly evolving AI regulation creates disproportionate uncertainty for SMEs lacking legal capacity and tailored guidance, increasing both non-compliance and over-compliance risks (Radu, 2021; OECD, 2024; Batool, Zowghi, & Bano, 2025).

Overall, these barriers reinforce one another: limited resources reduce experimentation and learning, which suppresses confidence and constrains investment. Breaking the cycle requires targeted external support, small pilot successes and education to build internal capability and trust.

5.2 Governance Challenges Specific to Consulting SMEs

Consulting SMEs operate in a context where knowledge-intensive work and personal trust constitute core value drivers. This context amplifies specific governance considerations when integrating AI:

- Preserving Human Expertise and Tacit Knowledge: Consulting relies on context-sensitive judgement that cannot be fully formalised; AI should therefore remain supportive rather than substitutive. Governance should enforce human-in-the-loop review for AI-assisted deliverables to protect the distinctive value of consulting advice (Schiff et al., 2021; Floridi et al., 2018);
- Client Trust and Transparency: AI can strengthen analytical rigour but can undermine confidence if its role is unclear or opaque. Material AI use should therefore be disclosed, and accountability for recommendations must remain explicit (Armour & Sako, 2020; Schiff et al., 2021);
- Data Confidentiality and Ethics: Given the sensitivity of client information, consulting SMEs need clear data boundaries, minimisation and secure processing environments; unsecured or public tools should be restricted for client data. Where safeguards cannot be ensured, AI deployment should be limited (Veale & Zuiderveen Borgesius, 2021);
- Maintaining Personal Service Quality: Excessive reliance on generic AI outputs may commoditise service and weaken the relational dimension. AI outputs should remain working material, with consultants shaping and contextualising final deliverables (Armour & Sako, 2020; Yang, Blount, & Amrollahi, 2024);
- Responsibility and Liability Clarity: Accountability does not shift to AI: consulting SMEs remain responsible for AI-assisted recommendations. Clear ownership, senior review and lightweight traceability support error handling and organisational learning without excessive burden (Schiff et al., 2021);
- Adaptive and Modular Governance Needs: For consulting SMEs, governance must remain proportionate: start with essential controls (data boundaries, human oversight and output quality) and expand modules as maturity grows, with periodic review to ensure practical fit (Batool, Zowghi, & Bano, 2025).

6 RESULTS AND DISCUSSION

Overall, the reviewed frameworks converge on lifecycle governance expectations (roles, oversight, documentation, and monitoring), but differ in their prescriptiveness and compliance burden (see Table 1–2). Mapped to enterprise risk governance (ISO 31000, COSO ERM and the Three Lines model), the analysis highlights a feasibility gap for consulting SMEs: comprehensive implementation is often unrealistic due to limited resources, data readiness and culture/trust constraints. To address this gap, we propose a modular, staged approach centred on a minimum viable set of controls that can be expanded as maturity grows (see Figure 1–2). This enables SMEs to capture AI benefits while maintaining client trust, accountability and service quality.

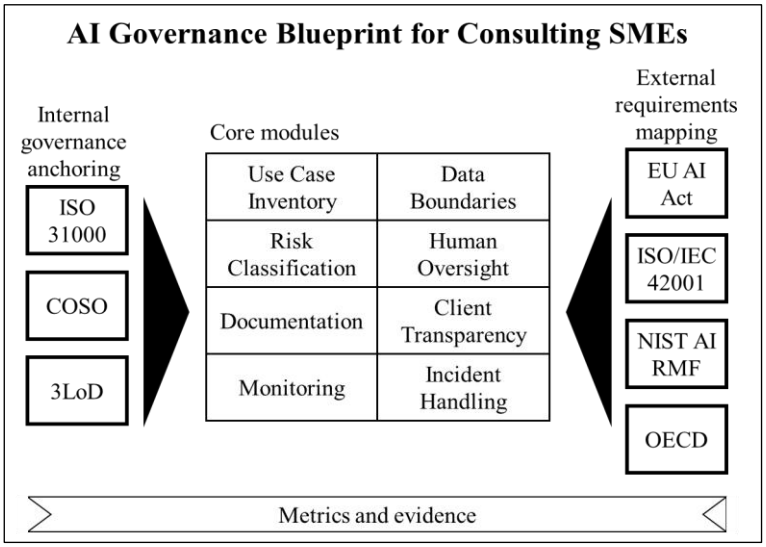

Figure 1 – Modular AI governance blueprint for consulting SMEs: Minimum viable modules and staged expansion (Source: Authors)

To operationalise the feasibility-first argument, the paper proposes a Modular AI Governance Blueprint for consulting SMEs (Figure 1). The blueprint defines a minimum viable set of governance modules (use-case inventory, data boundaries, role allocation, risk classification, human oversight, documentation and transparency, monitoring, and incident handling) that can be expanded as maturity grows. Each module is designed to map both to external governance expectations (regulation/standards) and to internal enterprise risk governance structures, enabling staged implementation without excessive bureaucracy. The blueprint's emphasis on concrete artefacts and role allocation aligns with enterprise architecture thinking that coordinates methodologies and ICT governance across the organisation (Helfert, Doucek, & Maryška, 2013).

Table 3 – Compact operational view of the modular AI governance blueprint (Source: Authors)

Module (Core)	Objective	Minimum Practice (SME)	Artefact	Role (3 Lines of Defence)	Metric/Proxy
Use Case Inventory	Visibility of AI usage	Record use cases and their purpose	AI Use Register	1st Line Owner	% of use cases recorded
Data Boundaries	Protection of data and clients	Data classification and defined "no-go" areas	Data Governance Rules	2nd Line (Policy)	Number of breaches/incidents
Risk Classification	Proportio-nality	Tiering (internal and legal)	Risk Assessment Note	2nd Line	% of high-risk cases with controls implemented
Human Oversight	Output quality	Defined review checkpoints	Review Checklist	1st Line + 2nd Line	Rework rate/error rate
Documentation	Auditability	Logging of "what / when / how"	Traceability Log	1st Line	Audit pass rate
Client Transparency	Trust	Disclosure rules	Client Disclosure Note	1st Line	Number of client escalations
Monitoring	Stability	Basic performance monitoring	Metrics Register	1st/2nd Line	Drift flags per month
Incident Handling	Responsive-ness	Incident logging and CAPA	Incident Record	2nd Line + 3rd Line	Time to close

Table 3 translates the dispersed requirements of major AI governance regimes into a single operational checklist designed for consulting SMEs. Instead of expecting SMEs to study and reconcile multiple frameworks, the figure decomposes governance into core modules and, for each module, specifies (i) the objective, (ii) the minimum practice that is feasible in a SME, (iii) a concrete artefact to produce, (iv) role allocation using the Three Lines model, and (v) a metric/proxy that can be tracked over time. The innovation is therefore not "another framework", but an implementation layer that makes existing frameworks actionable under real SME capacity constraints. In practice, this reframes governance from an abstract compliance exercise into a small set of evidence-based outputs that can be reviewed, improved and, if needed, audited.

To use Table 3, a consulting SME can start by selecting a specific AI use case, or a small set of use cases, and walking through the modules row-by-row as a staged implementation path. The firm first produces the minimum artefacts (e.g., a use-case entry, basic data boundary rules, and a traceability note for AI-assisted outputs), assigns ownership using a lightweight separation of duties (first line = project delivery team; second line = designated risk/compliance lead; third line = periodic internal or external assurance), and then tracks the suggested proxies to detect early drift, quality issues, or compliance gaps. This approach is intentionally modular: SMEs can adopt the minimum viable set quickly and extend modules later as maturity grows or as regulatory/client requirements increase. Since each

module defines both "what to do" and "what to show" (artefact + metric), governance becomes easier to operationalise without building a heavy bureaucracy.

The reason for introducing this blueprint is the feasibility gap demonstrated in the paper: comprehensive governance is often unrealistic for consulting SMEs due to limited resources, fragmented data readiness, and trust-based delivery models where reputational damage is costly. Table 3 directly targets these constraints by prioritising high-impact, low-burden controls that protect service quality and client trust while keeping the workload proportionate. In other words, governance becomes a quality and trust enabler: it reduces rework caused by unreliable AI outputs, supports consistent human oversight, and increases transparency and accountability in AI-assisted deliverables. By providing a minimum viable pathway with clear responsibilities and measurable indicators— Table 3 also offers a practical starting point for continuous improvement—SMEs can iterate based on metrics rather than relying on ad hoc judgement or attempting full-scale compliance implementations from day one.

7 CONCLUSION

In conclusion, AI governance and risk management are crucial for consulting SMEs not merely as compliance tasks, but as enablers of sustainable innovation and trusted service delivery. By adopting governance measures suited to their context, these firms can benefit from AI (efficiency, better insights, and new service offerings) while safeguarding the trust and professional accountability that define their brand. The reviewed foundations provide a starting point, but the challenge remains to bridge theory and practice through proportionate, implementation-ready governance that keeps the human element at the core.

By reframing AI governance as a feasibility problem, this paper moves beyond descriptive comparison and offers a structured rationale for a minimum viable governance set for consulting SMEs. The next step is operationalisation: turning the proposed logic into templates (e.g., AI use register, data classification rules, human-review checkpoints) and validating the approach in SME pilots under real client constraints.

ACKNOWLEDGMENTS

This work was supported by grant No. IP4040 – Support for Doctoral Research at Prague University of Economics and Business.

REFERENCES

Armour, J., & Sako, M. (2020). AI-enabled business models in legal services: From traditional law firms to next-generation law companies? *Journal of Professions and Organization, 7*(1), 27–46. https://doi.org/10.1093/jpo/joaa001

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. *AI and Ethics, 5*(3), 3265–3279. https://doi.org/10.1007/s43681-024-00653-w

Benraouane, S. A. (2024). *AI management system certification according to the ISO/IEC 42001 standard: How to audit, certify, and build responsible AI systems*. Abingdon, Oxon: Routledge.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Hurley, H., Crootof, R., Evans, O., Kaspersen, P., O'Heigeartaigh, S., & Amodei, D. (2020). *Toward trustworthy AI development: Mechanisms for supporting verifiable claims.* Proceedings of the AIES Conference. https://doi.org/10.48550/arXiv.2004.07213

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management—Integrating with Strategy and Performance.* New York, NY: COSO.

Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General, 144*(1), 114–126. https://doi.org/10.1037/xge0000033

European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

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: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Fraser, J. R. S., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons, 59*(6), 689–698. https://doi.org/10.1016/j.bushor.2016.06.007

Helfert, M., Doucek, P., & Maryška, M. (2013). The "Enterprise Architect" – A new approach to business informatics management. *Quality Innovation Prosperity, 17*(1), 67–87. https://doi.org/10.12776/qip.v17i1.171

Institute of Internal Auditors. (2020). *The IIA's Three Lines Model: An update of the Three Lines of Defense (Position paper).* Retrieved from https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

ISO. (2018). *ISO 31000:2018* R*isk management—Guidelines*. Geneva, Switzerland: ISO.

ISO/IEC. (2023). *ISO/IEC 42001:2023 Artificial intelligence—Management system*. Geneva, Switzerland: ISO.

Jobin, A., Ienca, M., & Vayena, E. (2019). *The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Three pathways for standardisation and ethical disclosure by default under the European union artificial intelligence act. *Computer Law & Security Review, 53*, 105957. https://doi.org/10.1016/j.clsr.2024.105957

Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes, 151,* 90–103. https://doi.org/10.1016/j.obhdp.2018.12.005

Maryška, M., Nedomová, L., & Doucek, P. (2020). Risk management and IT risk management processes and implementation: How Covid-19 has changed them. In J. Ministr (Ed.), *Proceedings of the 23rd International Conference on Information Technology for Practice (IT4P-2020)* (pp. 151–160). Ostrava, Czech Republic: Czech Society for Systems Integration.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys, 54*(6), 1–35. https://doi.org/10.1145/3457607

OECD. (2024). *Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449).* Retrieved from: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *Journal of Strategic Information Systems, 34*(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885

Radu, R. (2021). Steering the governance of artificial intelligence: national strategies in perspectives. *Policy and Society, 40*(2), 178–193. https://doi.org/10.1080/14494035.2021.1929728

Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Jost, J., & Barnes, D. (2020). Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*, 33–44. https://doi.org/10.1145/3351095.3372873

Sánchez, E., Calderón, R., & Herrera, F. (2025). *Artificial intelligence adoption in SMEs. Applied Sciences, 15*(12), 6465. https://doi.org/10.3390/app15126465

Schein, E. H. (2017). *Organizational Culture and Leadership* (5th ed.). Hoboken, NJ: Wiley.

Schiff, D., Rakova, B., Ayesh, A., Fanti, A., & Lennon, M. (2021). Explaining the Principles to Practices gap in AI. *IEEE Technology and Society Magazine, 40*(2), 81–94. https://doi.org/10.1109/MTS.2021.3056286

Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* Gaithersburg, MD: National Institute of Standards and Technology.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU AI Act. *Computer Law Review International, 22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Veber, J., Nedomová, L., & Doucek, P. (2016). Corporate Digital Incident Investigation. *Quality Innovation Prosperity, 20*(1), 57-71. https://doi.org/10.12776/qip.v20i1.656

Yang, J., Blount, Y., & Amrollahi, A. (2024). Artificial intelligence adoption in a professional service industry: A multiple case study. *Technological Forecasting and Social Change, 201*, 123251. https://doi.org/10.1016/j.techfore.2024.123251

ABOUT AUTHORS

Ludmila Jiříčková ORCID: 0009-0004-3761-0993 (L.J.) – Ing., doctoral researcher, The Department of Systems Analysis, Faculty of Informatics and Statistics, Prague University of Economics and Business, Czech Republic, e-mail: ludmila.malinova@vse.cz.

Petr Doucek ORCID: 0000-0002-5647-661X (P.D.) – full professor, Ing. CSc., Head of the Department, The Department of System Analysis, Faculty of Informatics and Statistics, Prague University of Economics and Business, Czech Republic, e-mail: doucek@vse.cz.

AUTHOR CONTRIBUTIONS

Conceptualisation, L.J.; Methodology, L.J.; Formal analysis, L.J.; Investigation, L.J.; Data curation, L.J.; Original draft preparation, L.J.; Visualisation, L.J.; Review and editing, P.D., L.J.; Supervision, P.D.

CONFLICTS OF INTEREST

The authors declare that they have no conflict of interest. The funders had no role in the design of the study, in the collection, analysis, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

DISCLOSURE

In the preparation of this manuscript, the authors used ChatGPT-5, a generative AI tool developed by OpenAI, for translation and language correction when translating text from Czech to English. The tool was used solely to improve linguistic clarity and ensure accurate translation (with the author's corrections afterwards), without generating or altering content. All intellectual and conceptual work remains the responsibility of the authors.