Journal of Engineering Management and Systems Engineering
https://www.acadlore.com/journals/JEMSE

Design and Evaluation of a Compliance Management Framework for Business Operations: A System Engineering Perspective

Tímea Antal[1*], Róza Számadó[2]

[1] Doctoral School for Safety and Security Sciences, Obuda University, 1081 Budapest, Hungary
[2] Donát Bánki Faculty of Mechanical and Safety Engineering, Obuda University, 1081 Budapest, Hungary

[*] Correspondence: Tímea Antal (antal.timea@uni-obuda.hu)

Received: 02-05-2026 **Revised:** 03-25-2026 **Accepted:** 04-03-2026

Citation: T. Antal and R. Számadó, "Design and evaluation of a compliance management framework for business operations: A system engineering perspective," *J. Eng. Manag. Syst. Eng.*, vol. 5, no. 2, pp. 120–136, 2026. https://doi.org/10.56578/jemse050201.

Abstract: Compliance management in business operations is often addressed through fragmented procedures that are difficult to coordinate and evaluate in a consistent manner. This study develops a structured compliance management framework grounded in a system engineering perspective, with the aim of linking regulatory requirements to operational processes in a coherent way. The framework is constructed by organizing compliance activities into a set of interrelated components, including regulatory interpretation, process integration, monitoring mechanisms, and feedback loops. On this basis, an evaluation scheme is established to examine the consistency and effectiveness of compliance implementation across operational stages. Particular attention is given to the identification of critical control points and the interaction between compliance measures and routine business processes. The proposed framework is examined through its application to typical organizational settings, where it allows a more transparent mapping between compliance requirements and operational execution. The analysis shows that a system-based structure supports clearer identification of process dependencies and facilitates more consistent evaluation outcomes. The study provides a structured basis for understanding compliance as an integrated operational system rather than a set of isolated practices, and offers a foundation for more informed decision-making in compliance management.

Keywords: Artificial intelligence; Compliance management; Organisational security; Risk management; Governance framework; Digital transformation

1 Introduction

In the 21st century, organisational adaptability and operational flexibility have become fundamental prerequisites for long-term business sustainability. Companies face increasing challenges due to the rapid diffusion of information and communication technologies, the growth of organisational data, and the transformation of work organisation and human resource management. In this environment, corporate compliance plays a critical role in risk mitigation, security assurance, and maintaining organisational resilience. As digital assets become central to business value, threats to their integrity, confidentiality, or availability directly affect organisational viability.

The widespread adoption of AI presents both opportunities and risks for corporate compliance. On the one hand, AI technologies—including machine learning and generative models—can enhance compliance processes through automated monitoring, predictive analytics, and decision-support systems, improving efficiency and reducing costs [1]. On the other hand, AI introduces new risks related to transparency, accountability, data bias, and legal responsibility [2, 3]. Unregulated or opaque use of AI may undermine organisational security and expose firms to compliance failures, financial penalties, and reputational damage [4]. These challenges are amplified by complex information and communication technologies infrastructures, including cloud computing and distributed systems, which complicate the integration of AI into existing compliance frameworks.

Although corporate compliance and AI have both been widely studied, they are often examined separately. Existing research provides insights into compliance management and AI governance individually, but empirically grounded frameworks that integrate AI into organisational compliance systems remain limited. This gap is particularly evident in practice, where regulatory expectations, technological capabilities, and security requirements intersect.

Both fields are interdisciplinary, drawing on economics, law, computer science, and organisational theory, and their regulatory environments continue to evolve, particularly in light of developments such as the EU AI Act.

From an organisational perspective, compliance systems and AI deployment share structural similarities. Both rely on structured standards and governance frameworks rather than fully comprehensive legal regulation (e.g., ISO/IEC 42001 and the National Institute of Standards and Technology AI Risk Management Framework), as highlighted in prior research on AI governance and system design [5], and both require organisational learning, technical expertise, and managerial commitment [6]. At the same time, AI adoption may affect corporate risk profiles. While implementation typically involves additional organisational investment and governance mechanisms, prior research suggests that these changes are closely linked to the need for increased oversight and accountability in AI-enabled systems [7]. Effective governance mechanisms may contribute to more consistent organisational processes and may be associated with improved operational efficiency and resilience over time [8].

This study addresses the identified gap by examining how AI tools are integrated into compliance processes and by developing a security-oriented organisational framework. Specifically, it investigates the risks and challenges associated with AI use and proposes structured solutions to support secure and lawful implementation.

The study is guided by the following research questions:

RQ1: What characteristics, risks, and applications can be observed in the integration of AI and compliance in organisations?

RQ2: What organisational solutions can enhance security awareness and support the secure use of AI?

Based on these questions, we hypothesise that AI adoption is positively associated with the formalisation of compliance processes and with higher levels of Organisational Security Awareness (SA).

1.1 Engineering Management and Systems Engineering Perspective

To analyse the intersection of AI and compliance, this study adopts an engineering management and systems perspective. Compliance is conceptualised not as a static set of rules but as a dynamic socio-technical control system.

Within this framework, the system boundary includes organisational units, AI models, data infrastructures, human actors, and regulatory requirements. Table 1 presents a systems view of AI-enabled compliance, describing inputs (e.g., regulatory mandates and data), processes (e.g., risk assessment and monitoring), outputs (e.g., compliance documentation), and feedback mechanisms (e.g., audits and performance tracking).

This perspective translates legal and ethical requirements into operational elements, enabling structured design, monitoring, and continuous improvement of compliance processes.

Table 1. Systems view of AI-enabled organisational compliance

System Component	Engineering Operationalization	Examples within AI Context
System boundary	The perimeter defining what is under organisational control versus external environments	Internal employee workflows, proprietary data stores, deployed AI models, Application Programming Interface endpoints
Inputs	Information, resources, or regulatory mandates entering the system	EU AI Act mandates, raw training data, generative artificial intelligence (GenAI) tool capabilities, vendor software updates
Processes	Mechanisms that transform inputs into desired outputs through functional decomposition	Continuous risk assessment, automated monitoring of model outputs, role-based employee training
Outputs	The tangible artifacts and behavioural changes produced by the system	Documented compliance evidence, mitigated risk profiles, automated incident reporting logs
Feedback loops	Sensing and actuation mechanisms designed to monitor outputs and adjust inputs/processes—Plan-Do-Check-Act (PDCA)	Internal audits, incident response protocols, model performance tracking, employee competence testing

Table 1 presents AI-enabled organisational compliance as a closed-loop system, illustrating the transformation of regulatory and organisational inputs into managed outputs through risk control, training, and feedback mechanisms. By reframing organisational governance as an engineered system, the proposed framework translates abstract legal and ethical principles into measurable design requirements, functional decompositions, and verification criteria, ensuring that AI deployment remains both innovative and strictly controllable.

2 Theoretical Framework

This study explores the relationship between compliance and AI with the objective of establishing a theoretical basis for the development of a management-oriented compliance tool. AI has become a significant driver of economic and organisational transformation. As highlighted by Brynjolfsson and his fellow researchers, the economic impact of AI is reflected in the growing demand for robotic equipment and intelligent devices, as well as in the increasing number of start-ups focusing on AI [9, 10]. Empirical and review-based studies further indicate that the integration of AI into production processes and corporate innovation activities leads to measurable growth at both organisational and industry levels [11, 12]. The macroeconomic and firm-level impacts of AI-based technologies, including their growth potential and productivity effects, are analysed extensively in the economic literature [13].

While the economic relevance of AI is widely acknowledged, its technological development has outpaced the evolution of ethical guidelines and legal regulation. The concept and technological complexity of AI systems evolve organically, driven by advances in data availability, computational power, and model architectures. Ethical and legal frameworks typically emerge as retrospective responses to technological change rather than as proactive governance mechanisms. In this context, the ethical guidelines developed by the EU High-Level Expert Group on AI define seven core requirements for trustworthy AI, including human agency and oversight, technical robustness, privacy and data governance, transparency, diversity and fairness, societal well-being, and accountability [14]. These requirements underline the necessity of organisational structures capable of translating abstract principles into operational controls.

The increasing reliance on big data and complex algorithmic models further amplifies governance challenges. As data volumes and model sophistication grow, the operational consequences of AI systems become more difficult to predict and interpret [15]. This opacity heightens the need for effective oversight mechanisms, risk management processes, and mitigation strategies to ensure that appropriate controls are in place throughout the AI lifecycle [16]. In response, standards and risk management frameworks play an increasingly important role. Practical guidelines, such as the National Institute of Standards and Technology AI Risk Management Framework, emphasise continuous risk identification, assessment, and mitigation from system design through deployment and operation [17]. The literature consistently highlights that ex ante risk management is more cost-effective and operationally efficient than addressing incidents after they occur [9, 18]. In this regard, security, data protection compliance, and legal conformity represent critical dimensions of organisational AI governance.

Despite the availability of ethical principles, standards, and risk management frameworks, organisational preparedness for AI remains limited. Few companies are fully equipped to manage the risks associated with the use of AI technologies. According to McKinsey's 2023 global survey, only 21% of respondents reported that their organisations had established formal policies governing the use of AI technologies by employees [10]. Longitudinal survey data collected between 2019 and 2023 further reveal a shifting risk landscape. In 2023, two new risk categories—system inaccuracy and intellectual property infringement—emerged among the most frequently cited AI-related risks, alongside previously identified concerns such as data protection and cybersecurity [10].

Taken together, the reviewed literature suggests that AI simultaneously functions as an economic opportunity and a source of novel organisational risk. This study builds on this conceptualisation by positioning compliance as a governance mechanism that integrates ethical principles, legal requirements, and risk management practices into the organisational use of AI. The resulting theoretical framework provides the foundation for analysing AI-supported compliance practices and for developing a structured compliance solution aimed at enhancing security awareness and supporting the responsible adoption of AI in organisational settings.

The study investigates the influence of AI adoption on organisational compliance practices and security awareness in Hungarian companies through a mixed methods research design integrating survey data and expert interviews. The findings demonstrate that AI use is associated with more formalised compliance processes and heightened security awareness, supporting the development of an adaptable, security oriented compliance framework that embeds AI into organisational monitoring, risk management, and decision support functions.

2.1 The Socio-Technical Systems (STS) Paradigm

To operationalise this approach, the study applies STSs Theory, which emphasises the interdependence of technical systems and organisational processes. AI systems are embedded in organisational contexts that include human decision-making, workflows, and governance structures [19].

From this perspective, effective AI governance requires coordination between technical controls and organisational practices. Concepts such as "social responsibility stacks" model governance as a feedback-based control system, enabling continuous monitoring and adjustment [18]. In practice, this involves managing interactions between human actors and technical systems, particularly in environments where AI adoption may introduce organisational friction [20].

2.2 Operationalizing Organisational Security Awareness

A key element of this loop is the human component. Despite the availability of ethical principles, standards, and risk management frameworks, organisational preparedness for AI remains heavily dependent on human competence. Empirical literature demonstrates that human behaviour poses a growing security risk, and while technical solutions are essential, they are insufficient to protect sensitive data against complex threats. For example, recent industry reports indicate a surge in GenAI usage, yet a majority of users report receiving no training on security or privacy risks, leading to the unauthorized sharing of sensitive workplace information with AI tools [21]. Furthermore, while 90 percent of organisations acknowledge that AI has increased general awareness, less than half of leaders feel their workforce is truly equipped to identify AI-specific threats [22].

Consequently, "security awareness" should be understood as a rigorous, multidimensional construct rather than a singular feeling of safety. Current research emphasises that SA encompasses knowledge acquisition, attitude formation, and behavioural execution [23]. The development of an Organisational Cybersecurity Awareness Scale has empirically validated that awareness is a four-dimensional factor consisting of personal, legal, technical, and policy-driven elements [24]. By conceptualising security awareness as an assessable engineering metric, organisations can diagnose vulnerabilities and deploy targeted interventions, transforming awareness from a compliance checkbox into a measurable defence mechanism. To drive actual culture change, organiations must shift toward behavioural metrics that track real-world executions rather than relying on static knowledge checks [16].

From a theoretical perspective, compliance is therefore conceptualised as a system that mediates the relationship between AI adoption and security outcomes. This theoretical framework provides the foundation for analysing AI-supported compliance practices and for developing a structured compliance solution aimed at enhancing security awareness and supporting the responsible adoption of AI in organisational settings.

3 Methodology

The development of an organisational compliance framework requires the systematic examination of both theoretical foundations and empirical practice. To establish a robust analytical basis, this study applied a mixed-methods research design combining quantitative and qualitative approaches. The research design was aligned with the theoretical framework of compliance and AI presented in the previous section.

3.1 Quantitative Data Collection

Quantitative data were collected using a structured questionnaire survey. The questionnaire was developed based on the theoretical foundations of compliance and organisational AI use and was administered online using Microsoft Forms. Data collection took place between 7 November 2024 and 16 December 2024 and followed a self-completion approach. A total of 139 valid responses were obtained. The questionnaire consisted of 35 items, including both closed-ended and open-ended questions. During data analysis, the response options "I do not know," "No answer," and "Not applicable" were treated as missing values and excluded from statistical processing. The number of valid responses was indicated separately for each item.

Table 2. Quantitative sample demographics (n = 139)

Demographic Category	Classification	Frequency (n)	Percentage (%)
Organisational role	Company managers	27	19.3
	Company owners	39	27.9
	Employees	74	52.9
Employee function (Subset n = 74)	Accounting	47	33.6
	Management-related	42	30.0
	Operational areas	27	19.3
	Information technology	13	9.3
	Marketing	5	3.6
	Administration	4	2.9
	Human resources	2	1.4
Company size	Micro or small (<50 employees)	111	79.3
	Medium (50–250 employees)	13	9.3
	Large (>250 employees)	16	11.4

The respondents represented Hungarian companies and included managers, owners, and employees. Of the respondents, 27 individuals (19.3%) were company managers, 39 (27.9%) were company owners, and 74 (52.9%)

were employees. Among the employees, 47 respondents (33.6%) worked in accounting, 42 (30.0%) in management-related functions, 27 (19.3%) in other operational areas, 13 (9.3%) in information technology, 5 (3.6%) in marketing, 4 (2.9%) in administration, and 2 (1.4%) in human resources. The units of analysis varied depending on the research question. In some analyses, the respondents themselves constituted the unit of analysis, while in other cases the unit of analysis was the organisation represented by the respondent. Each analysis clearly indicated the applied unit of analysis. Regarding company size, 79.3% of the organisations (111 companies) were classified as micro or small enterprises, 9.3% (13 companies) as medium-sized enterprises, and 11.4% (16 companies) as large enterprises. The sample cannot be considered representative of the overall size distribution of active companies in Hungary; therefore, the results should be interpreted as exploratory rather than generalisable. Statistical analyses were conducted using SPSS version 30.0 (SPSS Inc., Chicago, Illinois, USA) and Microsoft Excel. Table 2 shows a summary of the respondents' socio-economic and enterprise background.

3.2 Qualitative Data Collection

To complement the quantitative findings and to gain deeper insight into organisational practices and expert perspectives, qualitative data were collected through structured expert interviews. A total of ten structured interviews were conducted, each consisting of 15 predefined questions. The order of the questions was fixed, and responses to most questions were mandatory in order to ensure consistency and comparability across interviews. The interviews lasted between 60 and 80 minutes and were conducted using Microsoft Teams or the voice recording function of a mobile device. All interviews were recorded with the consent of the participants and subsequently transcribed verbatim into Microsoft Word for qualitative analysis.

In terms of demographic characteristics, five interviewees were between 40 and 50 years of age, three were between 30 and 40 years old, and two were between 50 and 60 years old. The gender distribution included nine male and one female participant. All interviewees held higher education degrees and occupied, or had previously occupied, senior or expert-level positions within their respective fields. The organisations represented by the interviewees operated in finance, security, information technology, healthcare, law, education, and research. Table 3 shows the educational and professional background of the professional respondents of the study. Table 4 shows the correspondence between questionnaire and interview.

Table 3. Qualitative interviewee demographics (n = 10)

Interviewee	Gender	Age Range	Professional Background	Current Position
1	Male	40–50	Historian, senior researcher	Professor
2	Male	50–60	Finance, accounting, economist	Head of department
3	Male	30–40	Information technology	Security technology specialist
4	Male	40–50	Electrical engineering, IT security	Senior IT risk manager, lecturer
5	Male	40–50	Programming	Digital coach in AI
6	Female	50–60	Law, economics	University associate professor, CEO
7	Male	40–50	Ethnography, cultural anthropology	Senior research fellow
8	Male	30–40	Economics	University associate professor
9	Male	30–40	Mathematical economics	Purchasing director
10	Male	40–50	Economics, sociology	Partner

Demonstrating the connection between the applied research methods and the resulting compliance framework is methodologically justified. Explicitly linking empirical findings to framework development enhances methodological transparency, strengthens the reliability and validity of the results, and supports the interpretability and reproducibility of the research. For this reason, the present study integrates quantitative and qualitative empirical evidence directly into the design of the proposed compliance framework.

The scope of the research does not include a conceptual or definitional analysis of compliance or AI. Instead, the study adopts established interpretations from the existing literature and focuses on organisational practice. The empirical investigation is therefore directed at understanding how compliance-related requirements and AI tools are currently applied within organisations, as well as identifying associated risks, governance gaps, and security challenges. The proposed compliance framework was developed inductively based on the insights gained

from the questionnaire survey and the structured expert interviews. The quantitative results provided an overview of organisational practices, levels of awareness, and recurring patterns, while the qualitative interviews offered contextualised explanations and expert interpretations of these findings. The triangulation of data sources enabled the identification of recurring compliance requirements and organisational needs relevant to the use of AI.

Table 4. Questionnaire and interview questions correspondence table

Questionnaire Question	Interview Question	Type of Correspondence	Category
What are the first three things that come to mind when you hear the terms compliance and AI?	What are the first three things that come to mind when you hear the terms compliance and AI?	Complete overlap	Compliance and AI concept
Does your company use any AI-based tools?	What AI-based usage habits and experiences do small and medium-sized enterprises (SMEs) have?	Complete overlap	Comparison of AI usage and experience
In which areas has your company used AI applications?	In which compliance areas can AI tools be used?	Partial overlap	Areas of AI application vs. compliance
Where within your organisation would you see the greatest benefit from using AI?	What responses can be given to new challenges in the area of compliance? Specific examples of difficulties in operating compliance? Are there any Hungarian or international best practices in compliance?	Partial overlap	Linking AI benefits and compliance responses
How do you assess the benefits and risks of using AI tools?	How can AI, which appears to be a risk, be turned into a compliance tool?	Partial overlap	Managing risks and opportunities from a compliance perspective
Does the company have compliance regulations?	How is the compliance approach present in Hungarian SMEs and what are its characteristics? What new conceptual elements could compliance have in the AI trend? What new functions could compliance have?	Complete overlap	The concept of compliance
How secure do you feel about AI tools in the workplace?	Is a checklist-type compliance sufficient for safe operation?	Partial overlap	Sense of security and effectiveness of compliance procedures
How are employees informed about compliance mechanisms?	What management methods can be used to integrate compliance into the organisational culture?	Partial overlap	The role of communication and management
What is the biggest challenge for management?	What is the biggest challenge for management? What specific changes could facilitate compliance operations?	Complete overlap	Management challenge
Please complete: “I use AI because...” and “...I don’t use AI because...”	How can compliance and AI be linked?	Complete overlap	Motivations and the connection between AI and compliance

Based on the empirical analysis, the compliance framework defines detailed organisational requirements and provides structured guidance across six core domains. These domains are: (1) compliance security policy, which establishes overarching principles and responsibilities; (2) the appointment of a designated person responsible for compliance implementation; (3) the development of an action plan with clearly defined milestones; (4) a comprehensive risk management strategy addressing AI-related risks; (5) the definition and documentation of organisational operations and business processes; and (6) the allocation of compliance resources and the

implementation of compliance awareness and training programmes. Together, these domains form an integrated organisational framework aimed at supporting secure, compliant, and responsible AI adoption.

3.3 Measures, Coding, and Construct Operationalization

Security awareness is defined in this study as a formative index; therefore, internal consistency measures such as Cronbach's alpha are not appropriate [25]. The construct consists of three theoretically distinct dimensions: (1) theoretical knowledge, (2) formal training exposure, and (3) observed or reported workplace behaviour. These dimensions are not interchangeable indicators of a latent construct but jointly define SA by capturing complementary aspects of organisational practice. As established in the methodological literature, formative indicators are not required to be correlated, as they collectively define the construct rather than reflect a single underlying factor [25].

3.3.1 Index construction and coding

To operationalize this construct, specific responses from the questionnaire were systematically coded and aggregated to form the composite index, adhering to standard practices for social science index construction [6].

Theoretical Knowledge was coded based on respondents' ability to identify multiple AI-related risks (e.g., financial, operational, IT/security, legal uncertainties). Responses were coded as a cumulative count, resulting in a continuous scale from 0 to 4.

Formal Training Exposure was derived from the reported frequency of IT security training. This was coded ordinally from 1 to 4 (1 = Less than once; 2 = Once a year; 3 = Twice; 4 = More than twice).

Workplace Behaviour and Culture was operationalized using the perceived safety and utility of workplace guidelines as a proxy for operational security posture. This was based on the 5-point Likert scale assessing how safe employees feel regarding AI tools in their workplace (1 = I do not feel safe at all, to 5 = I feel completely safe).

Because the component variables were measured on different scales, all variables were standardised using z-score transformation (μ = 0, σ = 1) prior to aggregation. This ensures comparability and prevents disproportionate influence of variables with wider numerical ranges [26].

3.3.2 Aggregation and weighting

The final SA index for each respondent i was calculated using a weighted linear combination of the standardized dimensions (Z):

$$\text{SA} = w1 \cdot Z1i + w2 \cdot Z2i + w3 \cdot Z3i$$

In the primary analysis, theoretically informed weights were applied based on the STSs literature. Because human behaviour and practical application are paramount in sociotechnical systems, Workplace Behaviour ($Z3i$) was assigned a weight of 0.40, while Theoretical Knowledge ($Z1i$) and Formal Training Exposure ($Z2i$) were each assigned a weight of 0.30. Utilising theoretical weighting schemes allows the composite indicator to accurately reflect the conceptual priorities of the research framework [27].

3.3.3 Robustness of the index

To ensure the index was not overly sensitive to the selected weighting scheme, alternative aggregation methods were tested and compared against the primary model. Specifically, an equal-weighting scheme ($w1$ = $w2$ = $w3$ = 0.33) yielded highly consistent index values (pairwise correlations > 0.90). In addition, excluding individual components of the index did not materially affect the main empirical results, indicating that the measure is not driven by any single dimension. Such sensitivity analyses are recommended to validate the structural integrity of composite indicators [27].

During the quantitative data analysis phase, response options such as "I do not know," "No answer," and "Not applicable" were strictly treated as missing values and handled via pairwise deletion to preserve sample integrity across specific variable relationships, thereby preventing the artificial skewing of the composite scores without discarding entire respondent records unnecessarily.

3.3.4 Qualitative coding and systems integration

For the qualitative data component, interview transcripts underwent a rigorous directed content analysis. The initial codebook was developed utilising highly specific terminology derived from STSs theory and international risk management frameworks (e.g., system boundary definitions, data integrity validation, human-in-the-loop dependencies, compliance formalisation protocols). Two expert researchers coded the extensive transcripts completely independently, identifying recurring thematic nodes related to AI risk archetypes, operational workflow bottlenecks, and systemic governance needs, subsequently resolving any minor inter-coder discrepancies through rigorous discussion and academic consensus to ensure absolute qualitative reliability.

The empirical findings suggest that the use of AI tools within the sampled Hungarian companies is associated with the emergence of more formalised compliance processes. Furthermore, the results indicate that integrating AI within structured organisational environments may support compliance practices and contribute to higher levels of SA.

A critical, paradigm-shifting analytical deduction from this study is that corporate compliance in the digital age should no longer be perceived as a static, policy-driven administrative obligation consisting of passive checklists. When viewed through the rigorous lens of STSs engineering, compliance operates as an active, continuously controllable management system. The findings support the interpretation of compliance as a socio-technical control system rather than a purely policy-driven function. Within this framework, the Plan-Do-Check-Act (PDCA) cycle provides a useful conceptual model for understanding feedback-oriented compliance processes, mirroring the Monitor-Analyse-Plan-Execute (MAPE-K) loops utilised in advanced software supply chain security. In this engineered context, the initial corporate policy creation and holistic risk assessment act as the fundamental Plan; the physical deployment of AI systems, functional process mapping, and active workforce training act as the Do; the continuous network monitoring, milestone tracking, and algorithmic auditing act as the Check (the critical sensing mechanisms); and the immediate corrective actions applied to mitigate identified vulnerabilities act as the Act (the responsive actuation mechanisms). This deep, systems-level operationalisation is explicitly designed to ensure that corporate compliance scales dynamically alongside aggressively evolving technological capabilities, ultimately preventing the organisation from becoming structurally brittle or legally exposed in the face of rapid, unpredictable AI advancement.

3.4 Statistical Procedures for Relational Analysis

Specific statistical procedures were employed to test the hypotheses regarding organisational AI use and compliance practices. All quantitative data processing and inferential testing were conducted using SPSS version 30.0. Bivariate Analysis of Categorical Variables.

To identify significant relationships between categorical variables—specifically, the adoption of AI tools (measured nominally) and the presence of formal compliance regulations (measured nominally)—Pearson's Chi-square (χ^2) test of independence was utilised. This test is the standard methodological approach in social science research for determining whether an observed association between two categorical variables is statistically significant or likely due to random sampling error [6].

3.4.1 Analysis of continuous constructs

To assess differences in the composite SA index across different operational groups (e.g., comparing the awareness scores of AI users versus non-users), Independent Samples t-tests were conducted. In instances where comparisons involved more than two categorical independent groups (e.g., evaluating security awareness across micro, medium, and large enterprises), a One-Way Analysis of Variance (ANOVA) was applied.

For all inferential statistical tests, the threshold for statistical significance was established a priori at α = 0.05. To evaluate the practical magnitude of the identified relationships and avoid over-relying on p-values, standard effect sizes—specifically Cramer's V for Chi-square analyses and Cohen's d for mean comparisons—were calculated alongside the primary test statistics.

4 Results

The empirical investigation focused on understanding how compliance-related requirements and AI tools are currently applied within organisations, identifying associated risks, governance gaps, and security challenges. The results demonstrate that the use of AI tools is significantly associated with ensuring compliance; companies that use AI tools are more likely to have formal compliance requirements than those that do not use AI. The chi-square test confirmed a significant association between the use of the device and the assurance of compliance (chi-square = 22.098, df = 1, $p < 0.001$). Based on Cramer's V coefficient, the association is of moderate strength (V = 0.424, $p < 0.001$).

4.1 Integrated Mixed-Methods Findings: Joint Display Analysis

To demonstrate how the qualitative evidence refines, challenges, and explains the quantitative patterns, the findings were integrated using a joint display table. In mixed-methods research, joint displays facilitate interpretation by structurally mapping survey data against interview themes, allowing for the explicit synthesis of system control needs. The qualitative interviews specifically isolated three distinct risk archetypes associated with AI: data authenticity and integrity, decision-making vulnerabilities, and a systemic lack of competence. Table 5 maps these qualitative insights directly to the survey findings.

The joint display analysis clearly confirms that compliance and AI are dynamic, mutually reinforcing factors within organisational architectures. The integration of AI generates new compliance challenges; however, resolving these challenges structurally contributes to an overall increase in SA, capability, and operational resilience. The interviews revealed that the role of compliance in managing AI risks is inherently three-dimensional: providing data protection guarantees, establishing process control frameworks, and executing competence development.

Table 5. Joint display of mixed-methods findings and system interpretations

Quantitative Finding (Survey)	Qualitative Theme & Representative Quote (Interviews)	Interpretation	Implication for Framework Domain
AI adoption & shadow IT: over 50% of respondents report using some form of AI tool (n = 75), primarily in marketing (50.7%), production (42.3%), and management (36.6%)	Unregulated usage & visibility: "Employees are using generative tools on their own devices without telling IT. The biggest challenge for management is visibility and establishing where our data is actually going."	AI adoption is occurring faster than formal governance structures can be implemented, creating invisible, porous system boundaries.	Domain I & V: urgent need for a formalized compliance security policy and clear mapping of business processes to establish definitive system boundaries
Compliance trigger: organisations utilising AI show a statistically higher likelihood of possessing formal compliance regulations (81.1%) compared to non-users	Risk reduction via process formalization: "When AI appears, it generates new compliance issues. We address this by institutionalising rules and adding control checkpoints into the everyday workflow."	AI acts as a forcing function for organisational maturity, requiring the transition from ad-hoc management to formalized systems engineering controls.	Domain II & III: requirement for a designated compliance officer and a structured action plan with measurable milestones to track maturity
Risk perceptions: legal uncertainties (21%), data protection (42%), and inaccurate decision-making rank (32%) as the highest perceived risks among respondents	Data integrity and algorithmic hallucinations: "The risk of data authenticity is massive. If we base financial forecasting on a hallucinated output, the liability is entirely on us. We need specific controls for AI output verification."	Technical risks in AI directly translate to business and legal liabilities, necessitating proactive threat modelling and continuous monitoring.	Domain IV: comprehensive risk management strategy focusing on algorithmic transparency, data lineage, and continuous feedback loops
Security awareness: High variance in perceived safety; however, regular training correlates positively with higher composite security awareness scores, using linear regression.	Competence deficits & human-in-the-loop: "The risk of a bad decision isn't just the algorithm; it's the lack of human competence in reviewing the output. Training cannot just be a checkbox; it must build real capability."	Security awareness is a product of continuous, relevant education and active socio-technical engagement, rather than static policy distribution.	Domain VI: allocation of compliance resources and implementation of role-based, continuous awareness training to build capability

4.2 Design Traceability: Evidence to Framework Mapping

In systems engineering, frameworks should be justified design artifacts with a traceable chain from evidence to design requirements. Table 6 provides a direct traceability matrix mapping the integrated empirical control needs identified in Section 4.1 to the specific framework requirements developed for the organisational system.

5 The Engineered Compliance Framework

Based on the empirical findings and the systems engineering design traceability matrix, the proposed compliance framework operates as a closed-loop system. The primary objective of the compliance framework is to legally and operationally ensure that companies can adapt to the dynamically evolving digital environment.

To overcome the limitations of text-heavy, policy-style documents that are difficult to operationalize, each of the six domains has been converted into a structured systems-engineering process template. These templates detail

the specific objectives, roles, inputs, process steps, outputs, control points, metrics, and review cycles required for implementation. The process steps within these templates actively incorporate the guidelines derived directly from the qualitative interviews and empirical data. The review cycles are explicitly grounded in the PDCA model, functioning as the feedback loops that ensure continuous system improvement.

Table 6. Framework design traceability matrix

Identified System Control Need (From Empirical Data)	Corresponding Framework Requirement	Systems Engineering Function	Verification Metric
Definition of acceptable AI usage and establishing system boundaries to prevent shadow IT	Domain I: compliance security policy	Baseline architecture & policy constraint	Percentage of workforce having signed the policy
Centralized accountability and resource allocation to manage rapid AI adoption	Domain II: appointment of a compliance responsible person	Governance routing & human oversight	Budget utilisation rate, formal appointment charter status
Structured deployment and continuous timeline tracking to mature AI processes	Domain III: action plan and milestones	Process sequencing & lifecycle management	Percentage of milestones achieved on schedule
Threat modelling, data integrity verification, and impact analysis for algorithmic risks	Domain IV: risk management strategy	Fault tolerance & system resilience	Incident frequency rate, number of mitigated vulnerabilities
Mapping AI tools to specific operational workflows to manage data inputs/outputs	Domain V: defining organisational operations	Functional decomposition & interface definition	Percentage of core processes fully documented with Interface Control Documents
Bridging the competence gap and standardizing human behaviour to ensure security	Domain VI: resources and awareness training	Human-system integration & capability building	Training completion rates; average competency test scores

5.1 Domain I: Compliance Security Policy

• **Objective**: To establish the overarching system boundary, defining acceptable AI use, data governance constraints, and legal conformity expectations across the organisation. This policy sets the architectural baseline for all socio-technical interactions.

• **Roles**: Executive Board (Approval), Chief Compliance Officer (Drafting and Enforcement).

• **Inputs**: Current regulatory frameworks (e.g., EU AI Act, General Data Protection Regulation, local labour laws), corporate strategic goals, existing IT security baselines, and industry standards (e.g., ISO/IEC 42001).

• **Process Steps**:

1) With the involvement of the relevant parties, develop a documented compliance security policy that provides a comprehensive overview of the requirements and the measures introduced or to be introduced.

2) Define the compliance security objectives, scope, roles, responsibilities, management commitment, framework for internal/external cooperation, and compliance criteria.

3) Ensure that the provisions of the compliance security policy comply with the laws, directives, regulations, standards, and recommendations applicable to the organisation.

4) Approve the policy and assume responsibility for the organisation's activities, assets, persons associated with the organisation, and risks considered significant.

5) Ensure that the compliance security policy is properly publicized, communicated, and applied in practice to guarantee effective implementation.

• **Outputs**: A documented, version-controlled Organisational Compliance Security Policy providing sufficient information to enable implementation consistent with the intent of the policy.

• **Control Points**: Mandatory policy acknowledgment by all employees before granting access to enterprise AI tools or network resources.

• **Metrics**: Percentage of the workforce having signed the policy; number of unauthorized AI tools blocked by network firewalls.

• **Review Cycle (PDCA)**: The current policy must be reviewed and updated at specified intervals, as well as following the occurrence of events such as findings from assessments, security incidents, or changes in applicable legislation (Check/Act).

5.2 Domain II: Appointment of the Compliance Responsible Person

• **Objective**: To designate centralized accountability for the continuous monitoring, maintenance, and enforcement of the AI compliance system, ensuring that human oversight is integrated into the governance architecture.

• **Roles**: Head of Organisation (Appointing Authority), Compliance Officer (System Owner).

• **Inputs**: Organisational chart, human resource budget, compliance security policy mandates.

• **Process Steps**:

1) The head of the organisation shall designate a person responsible for the operation of compliance. Ensure this person maintains an appropriate level of independence.

2) Empower the responsible person to coordinate, develop, implement, and maintain compliance with the organisational compliance security policy.

3) The head of the organisation shall ensure that the designated person has the resources necessary to achieve the objectives, which may include appropriate training, tools, technology, and support staff.

• **Outputs**: Formal appointment charter; allocated and approved compliance budget.

• **Control Points**: Bi-annual resource adequacy review by the Executive Board to ensure the Compliance Officer has sufficient capability to execute the mandate.

• **Metrics**: Time-to-resolution for reported compliance incidents; compliance budget utilisation rate.

• **Review Cycle (PDCA)**: Continuous operational authority, formally evaluated during annual performance reviews to adjust resources as needed (Act).

5.3 Domain III: Action Plan and Milestones

• **Objective**: To operationalize the compliance policy through a structured, measurable roadmap that aligns technical AI integration with risk management goals and business objectives.

• **Roles**: Compliance Officer (Lead), IT Management, Department Heads.

• **Inputs**: Compliance Security Policy, identified operational bottlenecks, technological procurement schedules, historical incident data.

• **Process Steps**:

1) Implement a procedure to ensure that compliance security and risk management measures and action plans are developed and maintained for the entire organisation.

2) Document remedial compliance security and risk management measures so that the organisation can respond appropriately to risks.

3) Ensure specified reporting requirements to management are met.

4) Document all steps and actions to ensure the transparency and traceability of the process.

• **Outputs**: Dynamic Compliance action plan; milestone tracking dashboards; remedial action logs.

• **Control Points**: Monthly status review meetings assessing milestone progress against baseline targets.

• **Metrics**: Percentage of milestones achieved on schedule; variance between planned and actual remediation times.

• **Review Cycle (PDCA)**: The action plan is updated quarterly based on an assessment of the measures implemented and continuous monitoring feedback (Check/Act).

5.4 Domain IV: Risk Management Strategy

• **Objective**: To systematically identify, evaluate, and mitigate risks associated with AI deployment, including algorithmic bias, data hallucinations, system inaccuracy, and intellectual property infringement, ensuring fault tolerance and system resilience.

• **Roles**: Chief Risk Officer/Compliance Officer, Data Stewards, System Owners.

• **Inputs**: Industry risk frameworks (e.g., National Institute of Standards and Technology AI Risk Management Framework), internal incident logs, proposed AI use-cases, system architecture models.

• **Process Steps**:

1) Develop a comprehensive risk management strategy, including processes for risk avoidance, transfer, reduction, and acceptance. Define the risk analysis methodology and risk values.

2) Align risk management with compliance and security management processes, as well as strategic and operational processes.

3) Identify and document assumptions regarding risks, risk management, and risk oversight. This includes priorities, organisational risk tolerance, and constraints.

4) Monitor and document risk management activities, including risk identification, assessment, and management.

5) Share the results of risk management activities with management and relevant stakeholders.

• **Outputs**: AI Risk Register; Threat Models; Mitigation Protocols; Risk Assessment Reports.

• **Control Points**: Go/No-Go gateway reviews prior to transitioning any AI model from testing to production environments.

• **Metrics**: Number of identified high-risk vulnerabilities; incident frequency rate; mitigation implementation speed.

• **Review Cycle (PDCA)**: Continuous monitoring of operational AI systems. The risk management framework criteria and strategy must be reviewed and updated at specified intervals to respond to organisational changes.

5.5 Domain V: Defining Organisational Operations and Business Processes

• **Objective**: To execute functional decomposition, explicitly mapping where and how AI tools interact with core business workflows, data pipelines, and human operators, establishing clear interface definitions.

• **Roles**: Process Owners, Systems Engineers, Compliance Officer.

• **Inputs**: Enterprise architecture diagrams, business continuity plans, departmental workflows, AI tool functional specifications.

• **Process Steps**:

1) Define organisational objectives and core functions, taking into account compliance security and the risks to organisational operations, individuals, and other organisations.

2) Define the compliance requirements arising from the organisational objectives and basic functions, understanding the harmful effects that compromising or damaging information can have.

3) Document the definitions of basic tasks, core functions, and the related protection requirements in accordance with organisational policies and procedures.

• **Outputs**: Documented process maps; Interface Control Documents; functional capability definitions.

• **Control Points**: Architectural review of process maps to ensure no "shadow AI" integration bypasses established data controls or system boundaries.

• **Metrics**: Percentage of core processes fully documented; frequency of unauthorized process deviations detected during audits.

• **Review Cycle (PDCA)**: Organisational objectives and core functions should be reviewed at specified intervals and modified as necessary to ensure their relevance and effectiveness in changing environmental and business conditions.

5.6 Domain VI: Compliance Resources and Awareness Training

• **Objective**: To build human-system resilience by elevating the composite security awareness (knowledge, attitude, behaviour) of the workforce interacting with AI, integrating human factors into the STS.

• **Roles**: Human Resources, Compliance Officer, IT Security Team.

• **Inputs**: Skill gap analyses, threat intelligence, updated compliance policies, user feedback.

• **Process Steps**:

1) Define the skills and abilities required to perform compliance tasks and develop role-based training programmes for those with compliance responsibilities.

2) Develop compliance career paths to encourage professionals to advance and institutionalise core competencies among staff.

3) Develop and deliver compliance awareness training to users, including the measurement of users' knowledge levels. Content should focus on the importance of security and the necessary protective measures.

4) Document the conduct of training (e.g., through attendance sheets and certificates) and the progress of participants to ensure continuous improvement.

5) Incorporate lessons learned from internal and external compliance events into the training materials and the compliance toolkit.

• **Outputs**: Training curriculum; attendance logs; competency assessment scores; compliance career development plans.

• **Control Points**: Automated restriction of AI tool access for employees who fail to complete mandatory training cycles or meet baseline competency scores.

• **Metrics**: Training completion rates; average competency test scores; reduction in human-error security incidents.

• **Review Cycle (PDCA)**: Training and awareness-raising materials should be regularly reviewed and updated to ensure content remains relevant, particularly following specific events or based on training feedback evaluations.

5.7 Practical Implementation Scenario: Small and Medium-Sized Enterprise Adoption of GenAI

To illustrate the practical applicability of the engineered framework, the following scenario outlines how a resource-constrained small and medium-sized enterprises (SME) can implement these domains during the adoption of GenAI tools for administrative and marketing workflows.

• Week 1–2 (Minimum Viable Action-Establishing Boundaries): Under Domain I & II, the SME Head appoints the IT Lead as the Compliance Responsible Person. They draft a one-page "Interim Generative AI Acceptable Use Policy" strictly prohibiting the input of personally identifiable information, confidential client financial data, or proprietary source code into public AI models. Control Point: The policy is circulated via the company's HR portal, requiring a mandatory digital signature acknowledgment from all staff before the end of the week.

• Day 30 (Process Mapping and Capability Building): Under Domain V, the Compliance Lead conducts functional decomposition of the marketing workflows. They explicitly define where GenAI can be used (e.g., drafting generic marketing copy) and where it is strictly banned (e.g., reviewing employee contracts). Under Domain VI, a 45-minute mandatory awareness session is held, focusing specifically on the risks of AI hallucinations and data leakage. Metric Tracked: 100% attendance and policy signature rate achieved.

• Day 60 (Risk Management Integration): Under Domain IV, the SME establishes a lightweight AI Risk Register. They identify a moderate risk that marketing copy generated by AI may infringe on copyright or contain fabricated statistics. Mitigation: A mandatory human-in-the-loop control is implemented—all AI-generated outward-facing content must be reviewed and approved by the Marketing Director before publication. This process is documented.

• Day 90 (Review and Audit Cycle): Under Domain III, the action plan milestone to establish baseline GenAI governance is marked complete. The Compliance Lead conducts a brief audit, checking network logs for usage of unauthorized AI platforms. The PDCA loop resets, using this feedback to plan training optimizations for the next quarter.

6 Discussion

The results indicate that the use of AI tools within Hungarian companies is associated with the emergence of more formalised compliance processes. Furthermore, the findings suggest that embedding AI within structured organisational environments may support compliance practices and may be linked to higher levels of SA.

One possible interpretation is that AI adoption necessitates greater procedural clarity, accountability, and oversight. As organisations integrate AI tools into their operations, they may need to establish clearer governance structures, particularly regarding data use, decision-making processes, and responsibility allocation. This perspective is consistent with the view that compliance can function as an active organisational mechanism that translates abstract regulatory requirements into operational practices.

From a systems perspective, the findings are consistent with interpreting compliance as a dynamic, feedback-oriented organisational system. In this context, structured processes such as continuous monitoring, auditing, and corrective actions may play a central role in maintaining alignment between technological deployment and regulatory requirements. Rather than being a static obligation, compliance may be understood as an adaptive organisational capability that evolves alongside technological change.

The mixed-methods design provides additional insight into this relationship. While the quantitative results indicate relatively high levels of AI adoption, the qualitative findings suggest that part of this adoption occurs informally, including practices that may be characterised as "shadow IT" [28]. These insights highlight a potential gap between formal governance structures and actual organisational behaviour. They also support the emphasis of the proposed framework on functional structuring (Domain V), continuous training (Domain VI), and proactive risk management (Domain IV) as mechanisms that may help mitigate the potential liabilities associated with algorithmic opacity [29].

From a practical perspective, the findings suggest that AI-supported compliance should not be viewed solely as a regulatory requirement but may also function as a mechanism that supports organisational stability and operational effectiveness. Prior research indicates that secure and well-governed AI implementation can contribute to measurable firm-level benefits [8]. In this context, integrating governance, training, and monitoring processes may help organisations reduce risks while supporting operational performance.

6.1 Inference Limits and Sample Representativeness

While the socio-technical principles reflected in the proposed framework—such as feedback-oriented control processes, structured functional decomposition, and human oversight—may have broader theoretical relevance, their practical implementation should be adapted to specific organisational contexts. Accordingly, the framework should

be interpreted as a conceptual and exploratory contribution, and its broader applicability requires further empirical validation.

Future research should prioritise cross-sectional, international, and longitudinal studies to assess the robustness and transferability of the observed patterns across different organisational environments and regulatory contexts.

The integration of these findings suggests that proactive AI compliance may function not only as a legal safeguard, but also as a structural element that can support organisational stability. However, any potential economic or performance-related benefits should be interpreted cautiously and in light of existing empirical evidence. For example, prior studies report modest firm-level value increases—achieving the 0.17% to 0.20% firm value—associated with secure AI integration [8], but the extent to which such effects can be generalised across organisational contexts remains uncertain.

The framework proposed in this study translates this economic potential by transforming abstract ethical guidelines into concrete, verifiable engineering metrics. While the empirical mixed-methods findings may support a highly robust structural foundation for the proposed engineered compliance framework, it is epistemologically imperative to explicitly acknowledge and delineate the strict limits of inference inherent in this study. The compiled dataset and resultant sample cannot be considered entirely representative of the global or macroeconomic corporate landscape, and the conclusions drawn could be interpreted by scholars and practitioners with appropriate scientific caution and contextual awareness.

Despite these contributions, several limitations should be acknowledged. First, the dataset is context-specific and focuses on Hungarian companies, which limits the generalisability of the findings. The sample (n = 139) is strongly skewed toward micro and small enterprises (79.3%), reflecting the structure of the national economy but limiting applicability to larger organisations.

Second, the statistical patterns identified throughout the analysis—such as the observed positive association between AI tool usage and the formal presence of compliance regulations—should be interpreted as exploratory, contextual correlations rather than as definitive, universal causal relationships or globally generalisable phenomena. Third, the resource constraints, inherent organisational agility, and existing IT infrastructures of micro-enterprises differ vastly and fundamentally from those of massive multinational conglomerates [30]. A large, heavily regulated global financial institution implementing autonomous, AI-driven algorithmic trading systems across multiple jurisdictions faces substantially different statutory burdens, capital market secrutiny, and systemic macroeconomic risks than a small, local marketing firm utilising publicly available GenAI solely for drafting promotional copywriting [31]. The economic impact of AI in large firms often involves complex human capital reallocation and significant capital market disruption, variables which are entirely absent in micro-enterprise operations [31]. Consequently, the applicability and impact of the proposed framework are likely to vary significantly across organisational types.

7 Conclusions

The scientific value of this research lies in its provision of practical guidance for businesses on effectively managing a compliance system. This study not only enriches the scientific discourse but also offers direct practical benefits; it aims to equip organisations to respond more adeptly to changes in the external digital environment, potentially allowing them to derive operational advantages from the synergies between compliance and AI.

This study makes several contributions to the fields of engineering management and systems engineering. First, the paper conceptualises organisational compliance explicitly as a managed STS, integrating regulatory requirements, organisational processes, and managerial control mechanisms. This extends existing compliance research by framing it as a dynamic, operationally embedded management system driven by continuous PDCA feedback loops. Second, the study introduces an integrated compliance framework that incorporates AI as both a functional system component and an object of governance. Third, by providing structured templates and a concrete implementation scenario, the paper translates abstract system design principles into actionable guidance for managers, overcoming the limitations of text-heavy policy documents.

Ultimately, cultivating a consciously engineered compliance culture may help ensure that AI acts as a catalyst for sustainable operational improvement rather than an uncontrolled vector of risk. Practical guidance, combined with a conscious organisational culture, ensures that compliance is not merely a formality but rather the cornerstone of long-term security, trust, and sustainable operation.

Author Contributions

Conceptualization, T.A.; methodology, T.A.; validation, R.S.; formal analysis, T.A.; investigation, T.A.; resources, T.A.; data curation, T.A.; writing—original draft preparation, T.A.; writing—review and editing, T.A.; visualization, T.A.; supervision, R.S. All authors have read and agreed to the published version of the manuscript.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] T. H. Davenport and R. Ronanki, "Artificial intelligence for the real world," *Harv. Bus. Rev.*, vol. 96, no. 1, pp. 108–116, 2018.

[2] C. Meske, E. Bunde, J. Schneider, and M. Gersch, "Explainable artificial intelligence: Objectives, stakeholders, and future research opportunities," *Inf. Syst. Manage.*, vol. 39, no. 1, pp. 53–63, 2022. https://doi.org/10.1080/10580530.2020.1849465

[3] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi *et al.*, "AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations," *Minds Mach.*, vol. 28, no. 4, pp. 689–707, 2018. https://doi.org/10.1007/s11023-018-9482-5

[4] ISACA, "Understanding the EU AI Act: Requirements and Next Steps," White Paper, 2024. https://complian cehub.wiki/content/files/2024/10/ISACA_Understanding_EU-AI-Act.pdf

[5] V. Vakkuri, K. K. Kemell, J. Kultanen, M. Siponen, and P. Abrahamsson, "Ethically aligned design of autonomous systems: Industry viewpoint and an empirical study," *arXiv preprint*, p. arXiv:1906.07946, 2019. https://doi.org/10.48550/arXiv.1906.07946

[6] E. R. Babbie, *The Practice of Social Research*, 15th ed. Boston, MA, USA: Cengage Learning, 2020.

[7] M. Iansiti and K. R. Lakhani, "Competing in the age of AI," *Harv. Bus. Rev.*, vol. 98, no. 1, pp. 60–67, 2020.

[8] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010. https://doi.org/10.2307/25750690

[9] E. Brynjolfsson, D. Rock, and C. Syverson, "Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics," in *The Economics of Artificial Intelligence: An Agenda*. Chicago, IL, USA: University of Chicago Press, 2019, pp. 23–57.

[10] M. Raj and R. Seamans, "Primer on artificial intelligence and robotics," *J. Organ. Des.*, vol. 8, no. 11, pp. 1–14, 2019. https://doi.org/10.1186/s41469-019-0050-0

[11] J. Furman and R. Seamans, "AI and the economy," National Bureau of Economic Research, Cambridge, MA, USA, Working Paper 24689, 2018. https://www.nber.org/system/files/working_papers/w24689/w24689.pdf

[12] U. Riemann and T. Ochs, "Machine learning get ready to measure the value for supply chain management: Understanding the value of machine learning in the context of business processes," in *Building Cloud Software Products: Innovation, Technology, and Product Management*. Cham, Switzerland: Springer Nature, 2025, pp. 111–128. https://doi.org/10.1007/978-3-031-92184-1_7

[13] A. Agrawal, J. Gans, and A. Goldfarb, *The Economics of Artificial Intelligence: An Agenda*. Chicago, IL, USA: University of Chicago Press, 2019.

[14] High-Level Expert Group on AI, "Ethics guidelines for trustworthy AI," European Commission, Brussels, Belgium, 2019.

[15] V. Mayer-Schönberger and K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston, MA, USA: Houghton Mifflin Harcourt, 2013. https://www.amazon.com/Big-Data-Revolution-Transform-Think/dp/0544227751

[16] McKinsey & Company, "The state of AI in 2023: Generative AI's breakout year," 2023. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year

[17] National Institute of Standards and Technology, "Artificial intelligence risk management framework (AI RMF 1.0)," U.S. Department of Commerce, Gaithersburg, MD, USA, NIST AI 100-1, 2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[18] O. A. Basir, "The social responsibility stack: A control-theoretic architecture for governing socio-technical AI," *arXiv preprint*, p. arXiv:2512.16873, 2025. https://doi.org/10.48550/arXiv.2512.16873

[19] R. Kalluri, "Socio-technical system challenges in the era of artificial intelligence: A comprehensive analysis," *Int. J. Bus. Manage. Stud.*, vol. 6, no. 9, pp. 75–91, 2025. https://doi.org/10.56734/ijbms.v6n9a8

[20] A. Amanollahnejad, S. Fosso-Wamba, M. S. Shabbir, and A. Pakseresht, "Aligning socio-technical systems: Rethinking AI adoption and digital transformation in SMEs," *Inf. Syst. Manage.*, vol. 43, no. 2, pp. 103–117, 2026. https://doi.org/10.1080/10580530.2025.2612175

[21] National Cybersecurity Alliance and CybSafe, "Oh Behave! The annual cybersecurity attitudes and behaviors report 2025s," Washington, DC, USA, 2025. https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2025

[22] Fortinet, "2025 Security Awareness Report: Why Training Works and Where Organizations Still Fall Short," Fortinet Training Institute, Sunnyvale, CA, USA, 2025. https://www.fortinet.com/uk/blog/industry-trends/2025-security-awareness-report-why-training-works-and-where-organizations-still-fall-short

[23] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014. https://doi.org/10.1016/j.cose.2013.12.003

[24] N. O. Ünsal and M. A. Ocak, "Development of organizational cybersecurity awareness scale (OCAS)," *Hacettepe Univ. J. Educ.*, vol. 41, no. 1, pp. 136–155, 2026. https://doi.org/10.16986/hunefd.1739282

[25] A. Diamantopoulos and H. M. Winklhofer, "Index construction with formative indicators: An alternative to scale development," *J. Mark. Res.*, vol. 38, no. 2, pp. 269–277, 2001. https://10.1509/jmkr.38.2.269.18845

[26] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 8th ed. Andover, Hampshire, UK: Cengage Learning, 2019.

[27] M. Nardo, M. Saisana, A. Saltelli, S. Tarantola, A. Hoffmann, and E. Giovannini, "Handbook on constructing composite indicators: Methodology and user guide," OECD, Paris, France, OECD Statistics Working Papers 2005/03, 2008. https://www.oecd.org/en/publications/handbook-on-constructing-composite-indicators-methodology-and-user-guide_9789264043466-en.html

[28] M. Silic and A. Back, "Shadow IT—A view from behind the curtain," *Comput. Secur.*, vol. 45, pp. 274–283, 2014. https://doi.org/10.1016/j.cose.2014.06.007

[29] B. Hohmann and G. Kollár, "Reflections on the data protection compliance of AI systems under the EU AI act," *Cogent Soc. Sci.*, vol. 11, no. 1, p. 2560654, 2025. https://doi.org/10.1080/23311886.2025.2560654

[30] C. Pelletier and L. M. Cloutier, "Conceptualising digital transformation in SMEs: An ecosystemic perspective," *J. Small Bus. Enterp. Dev.*, vol. 26, no. 6/7, pp. 855–876, 2019. https://doi.org/10.1108/JSBED-05-2019-0144

[31] D. Acemoglu, D. Autor, J. Hazell, and P. Restrepo, "Artificial intelligence and jobs: Evidence from online vacancies," *J. Labor Econ.*, vol. 40, no. S1, pp. S293–S340, 2022. https://doi.org/10.1086/718327

Nomenclature

GenAI	Generative artificial intelligence
MAPE-K	Monitor-analyze-plan-execute
PDCA	Plan-do-check-act
SME	Small and medium-sized enterprises

Appendix

Appendix 1. Questions Asked in the Questionnaire Entitled "Ompliance and AI Rresearch in the Hungarian SME Sector"

1. Name of the company?
2. Registered office of the company (name of town)?
3. Main activity of the company (TEÁOR'08)?
4. Who completed the questionnaire? (Please select one): manager/owner/other
5. What area do you work in within the organisation? HR/Marketing/Accounting/Management/Customer service/Administration/IT/Other professional tasks (e.g., engineer)
6. What is the size of the company? Micro or small enterprise (fewer than 50 employees)/Medium-sized enterprise (50–250 employees)/Large enterprise (more than 250 employees)
7. What are the three things that first come to mind when you hear the terms compliance and AI?
8. Does your company use any AI-based tools? Yes/No/I don't know

If you answered "Yes" to the previous question, which ones? (You can select more than one answer at a time):

Dall-E/ChatGPT/DeepL/Brickabrac AI/Gemini/Claude/Midjourney/Character AI/QuillBot/Microsoft Copilot/TensorFlow/SAP/Bard/Novel AI/CapCut/Janitor AI/Civitai/My answer to the previous question was "No"/Other

9. In which areas have you seen your company use AI-based applications/tools? (You can select multiple answers at once):

My organisation does not use such applications or tools/I am not involved/Accounting, bookkeeping/HR/Customer service, support/Administration/Marketing/Business development/Management/Other (e.g., production, market research)

10. Where within your organisation would you see the greatest benefit from using AI?
11. Please complete the sentence: "I use AI because..."
12. Please complete the sentence: "I don't use AI because..."
13. How do you rate the benefits of using AI tools? (Please rate each item):

It facilitates, simplifies, and speeds up work
It gives the business a competitive advantage
It improves organisational processes
It provides marketing opportunities
It increases adaptability
14. How do you assess the risks of using AI tools? (Please rate each item):
Financial constraints (e.g., total costs of implementation and operation)
Operational difficulties (e.g., lack of expertise)
IT and security challenges
Legal uncertainties
Lack of use cases
Other
15. Have you experienced any cyberattacks or similar incidents caused directly or indirectly by an AI-based tool? Yes/No
16. Are there user and security guidelines for the use of AI-based tools at your workplace?
If you answered "No" to the previous question, select the third option
Yes/No/I did not answer the previous question
If you answered "Yes" to the previous question, how appropriate and useful do you find these regulations for maintaining security?
Scale: I feel completely secure—I do not feel secure at all
17. How safe do you feel about the AI-based tools used at your workplace? Scale: I feel completely safe—I do not feel safe at all
18. How many times a year does your workplace hold IT security training or any other training related to this topic? Less than once/Once a year/Twice/More than twice/Other
19. How relevant and useful is this training? Scale: Completely relevant and useful—Not at all relevant or useful
20. Does your company have compliance regulations or policies? Yes/No/I don't know/Other
21. How often does your company review its compliance rules? Annually/Periodically/When a new risk factor arises/Never/I don't know/There are no such rules
22. What does your organisation currently use compliance rules for? (You may select more than one answer):
My organisation does not use them/Not applicable/To monitor changes in legislation/To manage training and certification requirements/For reputation purposes/To monitor and manage regulations and approvals/Other
23. How does your organisation inform employees, contractors, and other responsible persons about the company's compliance mechanisms? (You may select more than one answer):
Through training/Through internal regulations (e.g., code of ethics or AI tool usage guidelines)/Through internal communication/Through the use of an internal company website/By organizing awareness-raising events/Other
24. In which area of compliance would you use AI? My organisation does not use it/I am not involved/Risk management/Process monitoring/Reporting

Table A1. Main characteristics of interviewees

	Gender	Age	Education	Position
1.	Male	40–50	Historian, Doctor of the Hungarian Academy of Sciences, senior researcher	Professor
2.	Male	50–60	Finance, accounting, economist	Head of department
3.	Male	30–40	IT specialist	Security technology specialist
4.	Male	40–50	Electrical engineer, electronic information security manager	Senior IT risk management manager, lecturer
5.	Male	40–50	Programmer	Digital coach in the field of AI
6.	Female	50–60	Lawyer, economist	University associate professor, CEO
7.	Male	40–50	Ethnographer, cultural anthropologist, PhD	Senior research fellow
8.	Male	30–40	Economist, PhD	University associate professor
9.	Male	30–40	Mathematical economist	Purchasing director
10.	Male	40–50	Economist, sociologist	Partner