AI GOVERNANCE FOR SAFE RURAL AUTOMATION: GLOBAL SURVEY OF LITERACY, OVERSIGHT AND REGISTRATION PRACTICES

Ayoola Rilwan Lawal[1], Tarmol Koppel[2], Romans Putans[3]
[1] University of Latvia. [2] Tallinn University of Technology (TalTech), Estonia. [3] University of Latvia.
al24181@students.lu.lv, tarmo.koppel@taltech.ee, email: se11374@lu.lv

Abstract. As industries increasingly adopt artificial intelligence (AI) and automation in safety-critical workplaces, the pace of deployment has outstripped governance practices that ensure occupational safety and health (OSH). In many regulatory frameworks, risk classification is increasingly being embedded as mandatory, but it remains unclear how organisations operationalise these requirements in practice as these governance gaps are particularly significant in rural-relevant sectors such as agriculture, food processing, energy, and logistics in which robust AI literacy, oversight, registration, and data governance are essential to prevent harm and ensure safety, sustainable operation of increasingly automated engineered systems. A cross-sectional online survey was conducted with 227 respondents across 18 countries, covering diverse sectors and organisational sizes. Likert-scale items assessed the presence of high-risk and non-high-risk AI systems and the implementation of key governance practices. Descriptive statistics were used to characterise adoption patterns. Chi-square tests examined differences between EU and non-EU organisations, with Cramér's V used to assess effect size. High-risk (81.8%) and non-high-risk (79.3%) AI systems are widely used, with no significant differences between EU and non-EU. High implementation levels were reported for AI literacy (90.4%), human oversight (86.9%), and monitoring and reporting (83.2%). Lower implementation was observed for fundamental rights impact assessments (76.7%) and comprehensive data governance (80.4%), indicating potential OSH vulnerabilities. Significant regional differences favoured EU organisations in AI literacy (97.8% vs 83.9%, $p = 0.021$), AI system registration (93.3% vs 77.1%, $p = 0.029$), while no significant differences were found for other governance measures.

Keywords: AI governance, EU AI Act, socio-technical system, occupational health and safety, automation in the workplace.

1. Introduction

The workplace adaptation of digital technologies in recent decades has profoundly reshaped the design and governance of work systems, as automation, connectivity, and data-driven technologies have transformed how work is organised and controlled across sectors. In the scope of this broader transformation, Artificial Intelligence (AI) and automation are tightly integrated in safety-critical work systems across sectors, including agriculture, oil and gas, waste management, food processing, energy, and logistics, with profound implications for occupational safety and health (OSH). The scope of this technology's universal adoption is becoming unprecedented and beyond isolated applications [1; 2], decision-making and risk management. While these technologies improve productivity, reduce hazardous exposures, and support predictive risk management, they also introduce novel socio-technical vulnerabilities linked to opacity [3], data dependence [4], and the potential for systemic failures in tightly integrated work systems [5].

Regulatory developments, most prominently the European Union AI Act [6; 7], introduced risk-based classification [6; 8] and a layered regime of obligations for high-risk systems, including requirements for human oversight [9; 10], documentation [11], monitoring [12], and registration, among others [13; 14]. These obligations directly intersect with occupational safety and health concerns relating to how AI restructures risk, accountability, and equity in workplaces [15; 16].

Despite its profound impact on governance practices of work systems, prior empirical studies of AI governance in practice are primarily focused on big technological industries and mature digital environments [17]. Therefore, limited empirical evidence exists in our understanding of how organisations operationalise such governance requirements in day-to-day practice, particularly in rural-relevant sectors that often exhibit lower digital maturity and more constrained regulatory capacity [3; 18].

Taken together, this gap raises critical questions about whether current governance practices are sufficient to safeguard workers and communities in increasingly automated environments.

To address the gap, the study investigates the reported implementation of high-risk and non-high-risk systems and key AI governance practices, including AI literacy, human oversight, registration, monitoring and reporting, data relevance and representativeness, transparency and fundamental right

impact assessment (FRIA) in organisations operating safety-critical automation, with a focus on rural-relevant sectors. We conducted a global cross-sectional survey across 18 countries with a mix of representatives across several domains. The study examines: 1. The prevalence of high-risk and non-high-risk AI systems in organisational practice. 2. The extent to which key governance mechanisms are implemented across regions. 3. Differences between EU and non-EU organisations in reported AI governance practices aligned with emerging regulatory expectations.

By presenting cross-national evidence on how organisations say they apply key governance practices, this study helps explain how risk-based regulation and similar rules are taken up as everyday responsibilities in safety-critical workplaces, and it underlines how little is yet known about whether these duties are carried through into the actual control of work.

2. Materials and methods

2.1. Study design and research questions

The study adopts a combined research design consisting of a conceptual and regulatory analysis followed by an empirical cross-sectional survey. The conceptual component is based on a targeted review of scientific literature and regulatory frameworks, including the European Union AI Act, and applies elements of a concept analysis approach to clarify key constructs such as AI literacy, human oversight, and AI governance practices in socio-technical systems. This component provides the theoretical grounding and informs the operationalisation of variables used in the empirical phase. Further, the study employed a cross-sectional online survey design to obtain a global snapshot of AI governance practices in organisations using AI and automation for safety-critical or operationally critical tasks. Following the research methodological design, the study pursues three specific interrelated objectives.

1. Characterise the prevalence of high-risk and non-high-risk AI systems in organisations in rural-relevant and safety-critical sectors across multiple countries.
2. Assess the extent to which key AI governance practices-AI literacy initiatives, human oversight mechanisms, AI system registration, monitoring and reporting, data governance, and fundamental rights impact assessments-are implemented.
3. Explore whether organisations located within the EU, where the AI Act is being implemented, report different levels of governance maturity compared to organisations outside the EU.

Thus, the above objectives motivate the following research questions (RQs):

RQ1: To what extent are high-risk and non-high-risk AI systems deployed in organisations across sectors and regions?

RQ2: How widely are AI literacy, human oversight, registration, monitoring, data governance, and fundamental rights impact assessments implemented in practice?

RQ3: Are there statistically significant differences between EU and non-EU organisations in the implementation of these governance practices?

Addressing these questions contributes to understanding how regulatory concepts of risk, oversight, and rights protection translate into organisational routines in OSH-relevant contexts.

2.2. Sampling, Recruitment, Eligibility

Participants were employees and employers familiar with their organisations' use of AI-based automated systems, such as occupational safety and health (OSH) managers, compliance officers, engineers, data analysts, operations line supervisors, management staff, production managers, software developers, HR managers, and policymakers. A non-probability sampling strategy was applied, combining purposive and snowball sampling techniques. The survey was distributed via professional networks, OSH associations, professional social platforms, industry and sectoral unions, as well as through direct sharing among participants. The survey was distributed over the period of November 2025 to March 2026. No financial or material incentives were provided to participants. Eligibility criteria required that respondents: a) were at least 18 years old; b) were employed in, or closely affiliated with, an organisation deploying AI or automated systems in safety-critical or operationally critical contexts (e.g., agriculture, food processing, energy, logistics, manufacturing); c) had sufficient insight into

organisational practices to answer questions on AI deployment and governance; and d) agreed to voluntary participation without inducement.

A total of 227 respondents from a range of organisational sectors and sizes started the participation in the survey. The following exclusion and data cleaning criteria were applied, particularly on the missing substantial indicators of geographical location and those of AI deployment and governance sections: 74 respondents did not indicate the country of usual residence, which is a crucial indicator of this study, thus they were excluded from the sample and 26 respondents left incomplete responses (blanks) for the crucial inclusion criteria of AI systems used in the company and their managerial/governance practices. Thus, following the data cleaning and application of inclusion/exclusion criteria, 127 valid responses were retained for analysis (response retention rate: 55.9%). Of the final sample, 38 respondents (29.9%) were from EU countries and 89 respondents (70.1%) from non-EU countries. As the distribution is uneven, with a larger proportion of respondents from non-EU countries, it should be considered when interpreting results of comparative analysis between jurisdictions subject to the EU AI Act and those operating under different regulatory contexts. Also, because the sample represents 18 countries, the relatively small number of valid responses reflects the targeted recruitment of respondents with specific organisational knowledge. Still, the sample size (N127, confidence level 95%, margin of error ± 8.52%) is sufficient for the application of chi-square tests of association with moderate expected cell counts; however, given the non-probability sampling design, the findings should be interpreted as exploratory and indicative rather than statistically representative of the global population.

2.3. Survey Instrument

The survey instrument (complex questionnaire) was designed to capture both the presence of AI systems and the implementation of governance mechanisms aligned with emerging regulatory frameworks. See the list of questions attached to Annex 1. The survey included four main sections.

1. Organisational profile (Q1-Q7): Country, sector, organisational size (e.g., micro, small, medium, large), and whether the organisation operated primarily in rural, peri-urban, or urban contexts.
2. AI system deployment (Q8(1-15)-Q9(1-16)): Items asking whether the organisation used AI systems that met the definition of high-risk under the EU AI Act (e.g., safety components of regulated products or applications falling into Annex III categories) and whether non-high-risk AI systems were deployed.
3. Governance mechanisms (Q10-Q16): Likert-scale items (e.g., strongly disagree to agree strongly; or not implemented to fully implemented) assessing AI literacy initiatives (e.g., training, awareness programs, internal guidance); Human oversight structures (e.g., clear assignment of supervisory responsibility, escalation pathways, ability to override AI outputs); AI system registration and documentation practices (internal inventories, registers, or external registries where applicable); Monitoring and reporting mechanisms (incident logging, performance monitoring, near-miss analysis related to AI systems); Data governance (data quality checks, documentation of data sources, access control, data protection measures); Fundamental rights and impact assessments (e.g., assessments of privacy, discrimination, and rights risks associated with AI deployments).
4. Perceptions and challenges (Q17, Q18): Open ended questions about challenges regarding human-AI interaction at workplace and possible improvements to make AI more human-centred.

Instrument design was informed by the AI Act's requirements for high-risk systems, OSH guidance on automation, and existing analyses of human oversight and AI literacy.

Survey link (questionnaire) is available also at Lime survey platform, https://limesurvey.ttu.ee/limesurvey/index.php/747791.

2.4. Construction and Operationalization of Measures and Variables

Key variables were constructed and operationalized aligning them with specific survey items as follows:

- High-risk AI deployment: Indicator (yes/no/uncertain) based on respondents' self-reported use of AI systems that they identified as high-risk under the AI Act definition or analogous national guidance (survey Q8.1-Q8.15).

- Non-high-risk AI deployment: Indicator (yes/no/uncertain) for other AI systems used in the organisation that did not meet high-risk criteria (survey Q9.1-Q9.16).
- AI Governance/management practices: For each governance domain (AI literacy, human oversight, registration, monitoring, data governance, fundamental rights assessment) 5 point Likert-scale responses were coded 1 = not implemented/used to 5 = fully implemented/used (survey Q10-Q16).
- Region: Organizations were categorised as EU or non-EU based on the country, enabling comparative analysis of governance practices in jurisdictions directly subject to the AI Act versus others (survey Q3).
- Organisational characteristics: Size and sectors created to explore potential associations with governance maturity and AI deployment (survey Q4-Q7).

Given that all measures are based on self-reported organisational practices, the variables may be subject to respondent interpretation and self-reporting bias, e.g., the self-reported classification of AI systems as high-risk may be subject to interpretation variance. This limitation is considered in the interpretation of results. To mitigate this, definitions in the survey were aligned closely with Articles 6 and Annex III of the AI Act.

2.5. Data Collection Procedures

Data were collected via an online Lime survey platform compliant with general data protection and security standards, using encrypted transmission and secure storage. The survey link was distributed over several weeks through professional networks, professional social media platforms, and collaboration partners. Weekly follow-up reminder messages were sent to increase response rates, and more than one response from the same individual was filtered based on IP address and time stamps where identifiable. Respondents could complete the survey on PC, IOS and Android mobile devices.

2.6. Data Analysis

Data were exported to a IMB SPSS Statistics version 30 (SPSS) for cleaning and analysis. Descriptive statistics (frequencies, percentages, means, standard deviations) were used to characterise a) prevalence of high-risk and non-high-risk AI systems, and b) distribution of governance mechanisms across organisations and regions. Chi-square tests of independence were conducted to examine associations between regions (EU vs. non-EU) and binary indicators of governance implementation (e.g., whether AI literacy programs were in place). Cramér's V was used to estimate effect sizes for significant associations, enabling interpretation of the strength of regional differences. Furthermore, to explore potential confounding effects, we conducted a stratified cross-tabulation across organisational size and sector. Given the cross-sectional design, associations are interpreted as non-causal.

2.7. Ethical Considerations

The research was conducted in line with established ethical standards for survey studies. Participation was voluntary, and informed consent was obtained on the survey page before respondents could proceed to the survey items. No personally identifiable data was collected, and no organisational names were requested by participants to be disclosed. Country and sector data were reported in aggregated form to mitigate the risk of deductive disclosure and maintain participant anonymity. Data were stored on a secure, restricted-access server and retained only for the period necessary for analysis and publication. The study design and survey material are within the applicable national and institutional guidelines on research involving human participants.

3. Conceptual and Regulatory Background

3.1. AI in Safety-Critical Rural-Relevant Sectors

Research by Ghobakhloo [19] shows that the so-called Industry 4.0 technologies are associated with improved operational efficiency, process optimisation, and sustainability outcomes in digitally enabled production environments [20]. In safety-critical, rural-relevant sectors such as agriculture, construction, food and feed processing, and energy infrastructure, automation supported by data-driven methods is

increasingly used to enable precision management, predictive monitoring, and real-time coordination of complex operations [21- 24]. While these deployments can reduce direct exposure of workers to hazardous tasks and environments, they also reposition risks by embedding control in opaque models and distributed data infrastructures, raising concerns about new failure modes, concentration of power, and challenges for accountability and oversight [25; 15].

Rural and hinterland regions often host such safety-critical operations, including agriculture, food and feed processing, and energy distribution, where infrastructure constraints, workforce skills gaps, and distance from regulatory hubs can intensify governance challenges [26]. Studies also indicate that rural enterprises frequently lag in digital readiness and skills, even as they adopt increasingly complex automation and digital tools [26; 27]. In this context, accessible literacy initiatives, practical oversight structures, and straightforward registration and documentation processes become central to translating high-level European regulatory requirements into effective protection for workers and surrounding communities [16].

3.2. Risk-Based AI Regulation and High-Risk Systems

The European Union AI Act establishes a risk-based regulatory framework intended to protect health, safety, and fundamental rights while supporting innovation and legal certainty in the internal market [6; 28]. The Act differentiates between prohibited practices, high-risk systems, transparency obligations for certain systems, and minimal-risk systems, while also introducing a distinct regime for general-purpose AI models [28]. High-risk status arises primarily in two ways: (a) where an AI system is a safety component of, or constitutes, a product regulated under sectoral Union legislation, and (b) where an AI system is intended for a high-risk use case listed in Annex III [64].

For high-risk AI systems, the AI Act sets out strict requirements and accountability across the lifecycle. Core requirements include a risk management system [29], data and data governance [30], technical documentation [11], record-keeping [31], transparency and provision of information to users [32; 74], and accuracy, robustness, and cybersecurity [33; 64]. Traceability and accountability are further strengthened through registration and database obligations: registration is set out in Article 49, and the EU database for certain high-risk systems is established under Article 71 [37].

Although the AI Act is the EU law, its risk-based logic and compliance expectations are already shaping governance debates beyond Europe, particularly for organisations supplying systems into the EU market or operating across jurisdictions [28; 7]. Recent studies suggest that many organisations still struggle to translate high-level requirements into workable internal procedures, especially where systems are bundled vendor solutions or embedded in legacy infrastructures [38; 39].

3.3. AI Literacy as a Foundation for Governance

AI literacy can be understood as “a set of competencies that enables individuals to critically evaluate AI technologies; communicate and collaborate effectively with AI” [40]. It also includes the ability to understand AI capabilities and limitations, critically appraise AI-mediated outputs, and make informed decisions about their use [41; 42]. In workplace contexts, this means the staff can recognise when AI outputs may be biased, incomplete, or misaligned with legal and ethical constraints, and know when human judgment must override automated recommendations [43; 41]. In safety-critical settings, AI literacy becomes a prerequisite for meaningful human oversight as required under the EU AI Act, because only sufficiently trained personnel can effectively monitor, interpret, and, where necessary, intervene in or override high-risk AI systems [75; 44; 45]. Without this literacy, human oversight risks becoming a procedural formality, and organisations may fail to detect situations in which automated decisions conflict with occupational safety and health (OSH) obligations or fundamental rights [46; 15].

Empirical studies on oversight show that humans often struggle to perform supervisory roles effectively, including automation bias, algorithm aversion, and difficulty judging when to override AI recommendations [47-49]. Without adequate literacy, formal oversight roles risk becoming nominal, with deployers either over-trusting system outputs or disregarding them without sound justification [48]. AI literacy initiatives, together with clear governance processes and escalation pathways, are therefore central to the effectiveness of regulatory requirements on human oversight [76; 50].

AI is progressively integrated into many everyday technologies. However, the algorithm systems are often poorly understood, and users may be unaware they are interacting with AI [51-53]. As a result, it can be difficult to deploy these systems effectively and appropriately, and to evaluate their outputs with healthy scepticism [54]. This kind of misunderstanding can push regulation in the wrong direction [55] and leave the public disappointed when expectations are not met [54]. In addition, when people can see the output but do not understand how it is produced ("black box"), it becomes easier to misread what the AI is doing [53]. Even when systems are more transparent, uncertainty can still arise if deployers lack the technical knowledge needed for correct interpretation [56; 57]. This is a core reason AI literacy matters at both ends, among developers and among users.

3.4. Human Oversight in AI Governance

Human oversight now plays a critical role in how AI is governed. This is because it is the practical means by which organisations identify problems, make decisions on relying on output, and adequately intervene when harm might happen. Its primary aim is to prevent risks to health, safety, and fundamental rights through output correction within the high-risk regulatory framework under the EU AI Act [64]. At the same time, it continues the extended objectives of preventing the system from displacing human autonomy and building trust in AI systems. Thus, Article 14 requires that providers establish the technical and operational conditions for effective oversight [64]. This is complemented by Article 26(2) of the AI Act, which requires deployers to assign qualified persons with competence, training, and authority to support oversight when necessary [36]. Enqvist [10] characterises the AI Act as "breaking new ground by promoting the introduction of the first general and sharp worded human oversight requirement over AI systems in European law" (abstract). Furthermore, it frames the oversight framework around "what" is to be overseen, "when" oversight is to be exercised, and "by whom" [10].

Regulatory and scholarly discussions distinguish between different oversight configurations, including human-in-the-loop (HITL), human-on-the-loop (HOTL), and human-in-command models (HIC) [58; 77]. HITL configurations involve humans actively approving outputs [58; 50], often in high-stakes decision contexts such as medical diagnosis or safety-critical control rooms. The system produces an output, but a human must review, approve, or choose before the action is taken [60; 61]. HOTL, automated process, supervised by a human, with operators stepping in only when needed, intervening based on performance indicators, alerts, or anomalies-an arrangement commonly discussed in guidance on human oversight for industrial automation, autonomous vehicles, and complex infrastructures. HIC implies that the accountable authority holds total control at the system level, setting objectives, defining acceptable boundaries, deciding when the system can be used, and holding authority to pause/stop or withdraw it from operation.

Empirical evidence suggests significant limitations to the effectiveness of human oversight, including humans' cognitive constraints and automation bias. Therefore, this means that Article 14's success requires careful implementation that acknowledges these limitations and avoids overreliance on human oversight as a standalone safeguard.

3.5. Registration, Monitoring and Data Governance

Registration and documentation are fundamental mechanisms to make AI systems visible to regulators, workers, and the public, enabling traceability and accountability across their lifecycle [6]. The AI Act establishes EU-wide databases for certain high-risk systems [37], complemented by obligations on both providers and deployers to register eligible systems [6], maintain internal technical documentation [11], automatically generated logs [34], and records of serious incidents and corrective actions [36].

Monitoring and reporting mechanisms serve to identify performance degradation, bias, emergent hazards, or near misses, and to trigger corrective action [64; 62]. In OSH terms, AI-enabled monitoring can support proactive risk management, but only when it is embedded in a governance framework that respects workers' rights and is transparent about the purposes and limits of data collection.

Comprehensive data governance is a further cornerstone of AI Act compliance, encompassing data quality, representativeness, provenance documentation, role-based access controls, security measures, and mechanisms for redress when data misuse leads to harm [30; 63]. Weak data governance can undermine model performance, embed structural biases, and increase the likelihood of both safety

incidents and fundamental rights breaches, particularly where high-risk systems depend on complex, longitudinal datasets [64; 65]. Emerging evidence also indicates that small and medium-sized enterprises-especially those operating in rural or otherwise resource-constrained contexts-often rely heavily on data-intensive digital tools without corresponding formal data governance frameworks, creating uneven readiness for AI Act obligations and increased exposure to governance failures [39; 49].

3.6. Fundamental Rights and OSH in Automated Workplaces

The adoption of AI-mediated automation in rural-related and safety-critical environments enhances productivity and safety, but it also introduces new risks [66]. A recent study by Bowdler et al. [67] highlights how automation alters workplace risk in a way that is not a physical hazard. Apart from injury and exposure to hazards, there are less obvious ways workers get exposed to harm. Automated work systems can also cause rights-relevant harms-privacy intrusion, unfair treatment, and reduced worker agency, which can eventually undermine safety performance. In addition, Özkiziltan and Landini [68] highlight how it can lead to power imbalance, a threat to fundamental right and biased and intrusive behaviour at the workplace.

When monitoring becomes pervasive [71; 69; 73], and workers have no understanding why assigned specific tasks and performance evaluations feel arbitrary [78; 68], and when workers lose agency to slow down or stop unsafe work [79], the system may appear efficient while becoming less safe in practice [80]. Fundamental rights, therefore, function as practical safety conditions: they help preserve trust, reporting, and the capacity for timely human intervention [81; 68].

The dual functional use of digital monitoring lies in its supportive role for feedback and safety, and its controlling role as a logging and sensing system for performance management [69; 70]. Monitoring data may be mobilised to drive productivity, enforce targets, or enable disciplinary control, often overshadowing any nominal safety function [69; 70]. When workers experience monitoring as control, behaviours can shift toward resistance and "gaming" the system, alongside higher strain and counterproductive responses that can undermine safe work [69; 71]. Where speaking up or reporting is perceived as punitive, reporting declines and learning signals weaken [72]. Over time, pervasive surveillance can foster a sense of being watched and distrusted, with privacy concerns and reduced autonomy contributing to poorer well-being [69; 73]. Concerns also arise when workers have limited clarity about what is captured, how it is used, and how inaccuracies can be corrected [69].

Allocation and evaluation are other concerns. Automated tools used for shift assignment and performance rating can subtly intensify established inequalities and psychosocial risks, including intensified workload, reduced decision authority and unpredictable working time [67]. These systems often do not capture vulnerability directly; instead, they rely on proxies such as contract type, health limits or caring duties, which tend to track who is already vulnerable. As a result, the hardest and riskiest work, together with tight time pressure, can cluster on the same workers, while options to challenge unfair allocations or scores remain limited [67]. Safeguards such as clear rationale, accessible appeal procedures and documented correction routes are therefore not only a matter of fairness; they directly shape who is exposed to danger and how incidents are prevented [73]. These dynamics can be particularly pronounced in rural-related industrial contexts, where jobs are scarce, sites are geographically dispersed, and oversight is centralised [67]. Workers may depend on a single employer, hold seasonal contracts and face long travel distances and isolation, all of which weaken their ability to resist or exit. In such settings, governance that treats rights and OSH together should prioritise bounded monitoring based on necessity, the possibility to contest data-driven decisions, strong protection of the right to stop unsafe work, and clear responsibility for those who configure, modify and audit the systems that structure daily labour [67; 73].

4. Results

4.1. Sample Characteristics

227 respondents participated in the survey and after data cleaning $N = 127$ valid responses were retained for analysis (response retention rate: 55.9%). Respondents represented a range of professional fields, namely education, engineering, information technology, law, healthcare, finance, public administration, and safety management. Regarding the size of organisation, 41.7% in large organisations

(≥ 250 employees), 13.4% in medium-sized enterprises (50-249 employees), 22.8% in micro-enterprises (< 10 employees), and 11.0% in small enterprises (< 50 employees). The pool of respondents was distributed across EU (N = 38) and non-EU (N = 89) jurisdictions. Such distribution enables comparative analysis of governance practices between jurisdictions subject to the EU AI Act and those operating under different regulatory contexts. Given the cross-national scope (18 countries) and non-probability sampling approach, the sample should be interpreted as exploratory. While the distribution across sectors and organisational sizes supports analytical diversity, it does not allow for statistical representativeness at the global population level.

4.2. AI System Usage by Classification

Of the full sample, 79.3% respondents reported using at least one system they classified as a non-high-risk AI system in their organisation, and 81.8% reported the presence of at least one they classified as a high-risk AI system in their organisation. Table 1 below presents the distribution of self-reported AI system deployment, distinguishing between high-risk and non-high-risk systems as defined in the survey instrument. These variables correspond to binary survey items assessing whether organisations use AI systems falling within high-risk categories (aligned with the EU AI Act definition) or other AI applications. Deployment of chi-square test for comparative analyses indicated no statistically significant differences between EU and non-EU respondents in the presence of non-high-risk systems – $\chi^2(1) = 0.17$, $p = 0.679$, nor high-risk systems – $\chi^2(1) = 0.60$, $p = 0.438$. These findings suggest broadly comparable levels of AI system deployment across jurisdictions.

Table 1

AI system usage by classification

AI System Type	Usage Yes *n*, *%*	Usage No *n*, *%*	Total *N*	χ^2	*p*
Non-high-risk AI	92 (79.3)	24 (20.7)	116	0.17	.679
High-risk AI	99 (81.8)	22 (18.2)	121	0.60	.438

Note. χ^2 values reflect EU vs Non-EU comparisons

4.3. Implementation of AI Governance Practices

AI governance practices were codified as "implemented" from 4 or 5 on a five-point Likert scale. Across the full sample, reported governance practices were at relatively high levels across domains. The governance practices include: AI literacy (90.4%), human oversight (86.9%), monitoring and reporting (83.2%), data relevance and representativeness (80.4%), transparency and communication (80.6%), fundamental rights impact assessment (76.7%), registration of high-risk systems (84.8%). See Table 2.

Table 2

Self-reported implementation of AI governance practices

Governance Practice	Implemented *n*, *%*	Not Implemented *n*, *%*	Total *N*
AI Literacy	104 (90.4)	11 (9.6)	115
Human Oversight	93 (86.9)	14 (13.1)	107
Monitoring and Reporting	89 (83.2)	18 (16.8)	107
Data Relevance and Representativeness	78 (80.4)	19 (19.6)	97
Transparency and Communication	87 (80.6)	21 (19.4)	108
Fundamental Rights Impact Assessment	79 (76.7)	24 (23.3)	103
Registration of High-Risk Systems	89 (84.8)	16 (15.2)	105

These results indicate that a majority of respondents report the presence of formal governance mechanisms across all examined domains, with particularly high implementation levels observed for AI

literacy and human oversight. In contrast, comparatively lower levels are observed for fundamental rights impact assessments and data governance, suggesting potential areas of weaker institutionalisation.

4.4. EU vs non-EU Comparisons in AI Governance Practices

For the investigation of jurisdictional differences, chi-square tests of independence were conducted, and Cramér's V was used to indicate effect size. Table 3 presents the proportion of organisations reporting implementation of each governance practice, disaggregated by EU and non-EU groups, alongside statistical test results.

Table 3

Comparison of AI governance practices implementation between EU vs Non-EU organizations

Governance Practice	EU%	Non-EU%	χ^2	*df*	*p*	Cramér's V
AI Literacy	97.8	83.9	5.51	1	0.021	0.23
Human Oversight	90.9	84.3	0.93	1	0.335	0.10
Monitoring and Reporting	91.1	79.6	2.46	1	0.117	0.16
Data Relevance and Representativeness	84.6	78.3	0.56	1	0.455	0.08
Transparency and Communication	86.7	76.5	1.62	1	0.202	0.13
Fundamental Rights Impact Assessment	80.5	75.5	0.32	1	0.572	0.06
Registration of High-Risk Systems	93.3	77.1	4.78	1	0.029	0.23

Note. χ^2 values are Pearson chi-square statistics. Cramér's V is reported as a measure of effect size for 2×2 tables (.10, .30, .50 correspond to small, medium, and large effects, respectively)

Contextualizing the statistical test results, the chi-square statistic (χ^2) evaluates whether there is an association between jurisdiction (EU vs non-EU) and implementation of each governance practice. In this study, statistically significant results ($p < 0.05$) indicate that observed differences between groups are unlikely to be due to random variation. The degrees of freedom ($df = 1$) reflect the binary structure of the comparisons (EU vs non-EU; implemented vs not implemented), and the p-value indicates statistical significance with the strength of association captured by Cramér's V. Across the analysed practices, statistically significant differences between EU and non-EU organisations were observed only for AI literacy ($p = 0.021$) and registration of high-risk systems ($p = 0.029$), while all other governance domains showed no significant variation between jurisdictions.

AI literacy management as the governance practice showed a statistically significant association with the jurisdiction ($\chi^2 = 5.51$, $p = 0.021$), with EU organisations reporting higher implementation rates (97.8%) compared to non-EU organisations (83.9%). While the effect size is small-to-moderate ($V = 0.23$), the result suggests that AI literacy initiatives, often emphasised in regulatory and policy frameworks, are more consistently institutionalised within the EU contexts. This indicates a targeted influence of regulatory environments on workforce preparedness and oversight capability.

A statistically significant association was also found between the registration of high-risk AI systems and the jurisdiction ($\chi^2 = 4.78$, $p = 0.029$), with higher implementation reported by EU organisations (93.3%) compared to non-EU organisations (77.1%). As with AI literacy, the small-to-moderate effect size ($V = 0.23$) indicates that the difference is meaningful but not large. This finding is consistent with the explicit documentation and registration requirements of the EU AI Act, suggesting stronger alignment of EU-based organisations with formal compliance-oriented governance practices.

No statistically significant differences between EU and non-EU organisations were observed for other AI governance practices – human oversight, monitoring and reporting, data relevance and representativeness, transparency and communication, and fundamental rights impact assessment.

Taken together, the results indicate that while most governance practices are widely reported across both EU and non-EU organisations, statistically significant regional differences are limited to AI literacy and registration practices. The consistently small effect sizes further suggest weak associations, indicating that jurisdiction plays a limited role in explaining variation in these governance practices. This pattern suggests broadly similar levels of governance implementation across regions, with

regulatory context exerting a targeted influence on specific domains rather than shaping overall governance maturity.

4.5. Summary of Empirical Results

Overall, the data indicate a high reported presence rate of governance mechanisms across the EU and non-EU jurisdictions. High-risk AI systems (81.8%) and non-high-risk systems (79.3%) are widely deployed, with no statistically significant differences between regions. Reported implementation rates exceed 80% for most governance domains, with AI literacy (90.4%) and human oversight (86.9%) among the most prevalent practices. Statistically significant differences between the EU and non-EU organisations were observed only for AI literacy (97.8% vs 83.9%, $p = 0.021$) and registration practices (93.3% vs 77.1%, $p = 0.029$), both with small-to-moderate effect sizes, while implementation levels of other governance domains observed did not differ significantly between the EU and non-EU respondents. These findings indicate that while governance practices are broadly present across jurisdictions, regulatory influence may be more pronounced in specific domains directly emphasised by the EU AI Act.

Taken together, these results suggest the following: (a) self-reported use of high-risk and non-high-risk AI systems is common in both EU and non-EU jurisdictions, (b) most respondents indicate that key governance practices are present, and (c) statistically significant differences in governance practices emerge between EU non-EU only for AI literacy and registration with small-to-moderate effect sizes. These align clearly with the EU AI Act obligations.

The implication for RQ1-RQ3 is that these questions, as currently operationalised, are necessary but not sufficient for judging whether regulation contributes to safe rural and infrastructure-intensive automation. Future research should treat governance practices (literacy, oversight, registration, monitoring and reporting, transparency and communication, data relevance and representativeness and FRIA) as a layer of a multi-level safety control system rather than as standalone indicators of safety. Empirically, this calls for studies that pair governance variables with detailed descriptions of work organisation, local adaptations, and control structures in specific sectors, and that distinguish clearly between what is visible in documents and what is enacted in the field. Normatively, it suggests regulatory and organisational regimes that require evidence of this mapping-evidence that the obligations expressed in law and policy can be traced, step by step, into the interfaces, procedures, staffing patterns, and escalation routes that determine how people live and work with automated systems in the places where things can actually go wrong.

5. Discussion

The survey results show that many organizations now report doing the things that regulations most clearly ask of them: they say they have literacy initiatives, human oversight arrangements, monitoring and reporting, transparency measures, attention to data relevance, impact assessments, and registration procedures in place, often at very high rates. In relation to the study's RQ1, the data show that both high-risk and non-high-risk AI systems are already present in many participating organizations across a diverse mix of sectors and regions. For RQ2, respondents report widespread uptake of governance practices, with most of these measures endorsed at the upper end of the response scale. For RQ3, statistically significant differences between EU and non-EU respondents appear only for literacy and registration, with EU organizations more likely to report these practices, while oversight, monitoring, data relevance, transparency, and impact assessment show no significant regional differences. Taken together, these patterns suggest that formal governance work is becoming part of routine organizational responses to risk, and that emerging regulation may already be shaping some aspects of practice, particularly in EU settings.

What the data do not show is equally important. The survey contains no items that describe how these commitments are anchored in day-to-day control of work, no information about interface changes, redistribution of tasks between people and automated functions, escalation and override in abnormal situations, or how maintenance and experience from incidents reshape practice.

The instrument, therefore, gives a detailed picture of the surface that is most legible to regulators and auditors, and almost no picture of the control structures that determine how people truly remain safe around such systems. The binary thresholds used to classify practices as "present" or "absent" further

limit what can be inferred about the maturity, integration, or effectiveness of these arrangements in everyday work.

Framed in terms of "work-as-imagined" and "work-as-done", the instrument is almost entirely a probe of work-as-imagined. It documents how organizations say they govern systems, not how those arrangements alter the possibilities for action, error, and recovery in real work. That asymmetry is not a minor limitation; it is a structural finding. It suggests that the most readily measurable aspects of governance are those that can be formalized in policies, training claims, and documented procedures, which align closely with the categories emphasized in the current EU AI regulation. The hard part, which is missing from the dataset, is the translation of these commitments into concrete constraints and supports in local work systems. The survey demonstrates how readily governance can be framed and evaluated without reference to it. The sector mix in the sample sharpens this concern. Respondents include engineers, process safety specialists, petroleum engineers, healthcare professionals, and practitioners in energy, oil and gas, logistics and transport, construction, water treatment, and related domains. In many such sectors, the technical systems that can cause the most harm, such as pipelines, substations, depots, treatment plants, and remote facilities are located in rural or peri-urban areas, while legal, administrative, and compliance functions sit in urban offices. Automation in these settings is therefore not limited to the agricultural sector; it spans remote monitoring, control, fault detection, and decision support across geographically dispersed assets. This spatial and organisational split makes them a particularly unforgiving environment for shallow governance. Paper-strong but operationally weak controls are most likely to be exposed when supervision is distant, local staffing is thin, and recovery from failure is slow. The survey does not identify rural deployments directly, so "rural automation" here is an analytic category that groups together automation embedded in dispersed, infrastructure-intensive work systems, rather than a labelled subgroup in the data. Even so, the sample composition is sufficient to justify treating such systems as a central use case for interpreting the results.

Against this backdrop, the call for compliance translation can be specified more tightly. It is not enough to note that obligations should be implemented. For the sectors represented here, translation can be assessed only if organizations can show how regulatory requirements map onto specific elements of the control loop: which interfaces were changed, which tasks were reassigned, which escalation paths were created or simplified, which override mechanisms were introduced or redesigned, how maintenance regimes were altered, and how near-miss and incident information is fed back into both governance documents and frontline procedures. None of this can be inferred from binary yes/no responses on literacy, oversight, or registration.

The observed differences in literacy and registration between the EU and non-EU respondents are consistent with regulation beginning to shape some aspects of practice, but they remain ambivalent until they are connected to tangible changes in how work is structured and controlled. The implication for RQ1-RQ3 is that these questions, as currently operationalized, are necessary but not sufficient for judging whether regulation contributes to safe rural and infrastructure-intensive automation. Future research should treat governance practices (literacy, oversight, registration, monitoring and reporting, transparency and communication, data relevance and representativeness, and FRIA) as a layer of a multi-level safety control system rather than as standalone indicators of safety.

In this study, the uniformly high reported implementation rates across multiple governance domains, combined with limited variation between EU and non-EU organizations, reinforce the need to distinguish between the presence of governance structures and their functional effectiveness in real work environments. Empirically, this calls for studies that pair governance variables with detailed descriptions of work organization, local adaptations, and control structures in specific sectors, and that distinguish clearly between what is visible in documents and what is enacted in the field. Normatively, it suggests regulatory and organizational regimes that require evidence of this mapping-evidence that the obligations expressed in law and policy can be traced, step by step, into the interfaces, procedures, staffing patterns, and escalation routes that determine how people live and work with automated systems in the places where things can actually go wrong.

Conclusions

The results indicate that AI systems are already widely present across organisations, with 81.8% of respondents reporting usage of high-risk systems and 79.3% reporting using non-high-risk systems. At

the same time, a high proportion of organisations report implementing governance practices, including AI literacy (90.4%), human oversight (86.9%), monitoring and reporting (83.2%), and registration of high-risk systems (84.8%). These findings suggest that formal AI governance mechanisms are becoming part of routine organisational practice across sectors and regions.

Differences between EU and non-EU organisations are limited. Statistically significant differences are observed only for AI literacy (97.8% vs 83.9%, $p = 0.021$) and registration of high-risk systems (93.3% EU vs 77.1%, $p = 0.029$), while no significant differences are found for human oversight, monitoring, data governance, transparency, or fundamental rights impact assessment. EU-based organizations are more likely than non-EU organizations to report AI literacy initiatives and system registration, suggesting that emerging regulatory frameworks, such as those in the EU, may already be shaping specific governance domains, but do not yet translate into broader differences in reported governance practices. However, the results are based on self-reported data and primarily reflect the presence of formal governance arrangements, such as policies, procedures, and training initiatives. They provide limited insight into how these arrangements are embedded in day-to-day work processes, decision-making structures, and operational control, particularly in dispersed and infrastructure-intensive environments typical of rural and safety-critical systems.

As a result, the current operationalization of RQ1-RQ3 is not sufficient for assessing whether regulatory frameworks meaningfully enhance safety in rural and distributed automation contexts. Governance mechanisms such as literacy, oversight, and registration should be understood as one layer within a broader safety control system that must be mapped to concrete changes in user interfaces, task allocation, escalation pathways, and feedback processes.

Future research should integrate organisational governance measures with detailed analysis of work-as-done, including how AI systems are used, monitored, and overridden in real operational contexts. This approach is necessary to ensure that evaluations of AI governance reflect both formal compliance and its practical realisation in environments where system failures can have significant safety consequences.

Author contributions

Conceptualization, A.R.L.; methodology, A.R.L.; validation, A.R.L.; formal analysis, A.R.L., T.K., R.P.; investigation, A.R.L.; writing-original draft preparation, A.R.L.; writing-review and editing, T.K., R.P.; visualization, A.R.L. and R.P.; project administration, A.R.L.; funding acquisition, A.R.L. All authors have read and agreed to the published version of the manuscript.

Funding

This research article is part of an A.R.L. ongoing PhD programme in Human Factors, Occupational Safety and Health, University of Latvia. The study project received funding from the University of Latvia under the postgraduate support program. The opinions expressed reflect only the authors' views.

Conflicts of interest

The authors declare no conflict of interest.

AI usage

The authors acknowledge the use of generative AI tools, including Perplexity (GPT5.1) for language refinement and Grammarly for proofreading. These tools were used only to improve readability and correct minor errors. All substantive intellectual contributions, including the development of the research questions, methodology, analysis, and conclusions, are the work of the authors.

References

[1] Dwivedi Y.K., Hughes L., Baabdullah A.M., Ribeiro-Navarrete S., Giannakis M., Al-Debei M.M., et al. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, vol. 66, 2022, 102542. DOI: 10.1016/j.ijinfomgt.2022.102542

[2] Spencer D.A. AI, automation and the lightening of work. AI & Society, vol. 40, No 3, 2025, pp. 1237-1247. DOI: 10.1007/s00146-024-01959-3
[3] Raji I.D., Smart A., White R.N., Mitchell M., Gebru T., Hutchinson B., Smith-Loud J., Theron D., Barnes P. Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency, 2020, pp. 33-44. Association for Computing Machinery. DOI: 10.1145/3351095.3372873
[4] Amodei D., Olah C., Steinhardt J., Christiano P., Schulman J., Mané D. Concrete problems in AI safety. arXiv, 2016. Available at: https://arxiv.org/abs/1606.06565
[5] Leslie D. Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute, 2020. Available at: https://www.turing.ac.uk/research/publications/understanding-artificial-intelligence-ethics-and-safety
[6] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 2024. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
[7] Veale M., Zuiderveen Borgesius F.J. Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International, vol. 22, No 4, 2021, pp. 97-112. DOI: 10.9785/cri-2021-220402
[8] Schuett J. Risk management in the Artificial Intelligence Act. European Journal of Risk Regulation, vol. 15, No 2, 2024, pp. 367-385. DOI: 10.1017/err.2023.1
[9] AI Act Service Desk. Article 14: Human oversight. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-14
[10] Enqvist L. "Human oversight" in the EU Artificial Intelligence Act: What, when and by whom? Law, Innovation and Technology, vol. 15, No 2, 2023, pp. 508-535. DOI: 10.1080/17579961.2023.2245683
[11] AI Act Service Desk. Article 11: Technical documentation. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-11
[12] AI Act Service Desk. Article 72: EU database for high-risk AI systems listed in Annex III. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-72
[13] AI Act Service Desk. Article 49: Registration. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-49
[14] European Parliamentary Research Service. Artificial intelligence act: Obligations for high-risk AI systems (EPRS IDA(2024)690690). European Parliament, 2024. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/690690/EPRS_IDA(2024)690690_EN.pdf
[15] Shah I.A., Mishra S. Artificial intelligence in advancing occupational health and safety: An encapsulation of developments. Journal of Occupational Health, vol. 66, No 1, 2024, uiad017. DOI: 10.1093/joccuh/uiad017
[16] Fisher E., Flynn M.A., Pratap P., Vietas J.A. Occupational safety and health equity impacts of artificial intelligence: A scoping review. International Journal of Environmental Research and Public Health, vol. 20, No 13, 2023, 6221. DOI: 10.3390/ijerph20136221
[17] Putans R., Zeibote Z. Public services client-accordance through coproduction and digitalization. European Studies: The Review of European Law, Economics and Politics, vol. 8, No 1, 2021, pp. 121-147. DOI: 10.2478/eustu-2022-0069
[18] Rakova B., Yang J., Cramer H., Chowdhury R. Where responsible AI meets reality: Practitioner perspectives on enablers for shifting organizational practices. Proceedings of the ACM on Human-Computer Interaction, vol. 5, CSCW1, Article 7, 2021, pp. 1-23. DOI: 10.1145/3449081
[19] Ghobakhloo M. Industry 4.0, digitization, and opportunities for sustainability. Journal of Cleaner Production, vol. 252, 2020, 119869. DOI: 10.1016/j.jclepro.2019.119869
[20] Dubickis M., Putans R., Hovlanne Z. Method for assessing organizational readiness to innovate in clothing and textile industry: Insights towards circular economy. Journal of Open Innovation: Technology, Market, and Complexity, 2025, 100665. DOI: 10.1016/j.joitmc.2025.100665

[21] Sekar S., Rajesh S., Sekar S.D. Artificial intelligence and machine learning approaches for smart agriculture. Agrarian economy and rural development - Trends and challenges. International Symposium, 15th edition, 2024, pp. 24-31. The Research Institute for Agricultural Economy and Rural Development (ICEADR). Available at: https://hdl.handle.net/10419/319502
[22] Agrawal K., Goktas P., Holtkemper M., Beecks C., Kumar N. AI-driven transformation in food manufacturing: A pathway to sustainable efficiency and quality assurance. Frontiers in Nutrition, vol. 12, 2025, 1553942. DOI: 10.3389/fnut.2025.1553942
[23] Smith O.J.M., de Mendonça F. AI-driven predictive maintenance framework for fault detection in smart grid and renewable energy systems. Journal of Electrical Electronics and Automation Technologies, vol. 1, No 2, 2025, pp. 42-49. DOI: 10.17051/JEEAT/01.02.06
[24] Dhal S.B., Kar D. Leveraging artificial intelligence and advanced food processing techniques for enhanced food safety, quality, and security: A comprehensive review. Discover Applied Sciences, vol. 7, 2025, 75. DOI: 10.1007/s42452-025-06472-w
[25] Ashrafi N., Yousefi S., Aby G.R., Issa S.F., Darabi H., Alaei K., Placencia G., Pishgar M. AI-driven solutions to improve safety and health: Application of the REDECA framework for agricultural tractor drivers. PLOS Global Public Health, vol. 5, No 6, 2025, e0003543. DOI: 10.1371/journal.pgph.0003543
[26] Ferrari A., Bacco M., Gaber K., Jedlitschka A., Hess S., Kaipainen J., Koltsida P., Toli E., Brunori G. Drivers, barriers and impacts of digitalisation in rural areas from the viewpoint of experts. Information and Software Technology, vol. 145, 2022, 106816. DOI: 10.1016/j.infsof.2021.106816
[27] Thomä J. An urban-rural divide (or not?): Small firm location and the use of digital technologies. Journal of Rural Studies, vol. 97, 2023, pp. 214-223. DOI: 10.1016/j.jrurstud.2022.12.020
[28] European Commission. AI Act. Shaping Europe's digital future. [online] [01.03.2026]. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[29] AI Act Service Desk. Article 9: Risk management system. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-9
[30] AI Act Service Desk. Article 10: Data and data governance. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-10
[31] AI Act Service Desk. Article 12: Record-keeping. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-12
[32] AI Act Service Desk. Article 13: Transparency and provision of information to deployers. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-13
[33] AI Act Service Desk. Article 15: Accuracy, robustness and cybersecurity. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-15
[34] AI Act Service Desk. Article 18: Documentation keeping. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-18
[35] AI Act Service Desk. Article 19: Automatically generated logs. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-19
[36] AI Act Service Desk. Article 26: Obligations of deployers of high-risk AI systems. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-26
[37] AI Act Service Desk. Article 71: EU database for high-risk AI systems listed in Annex III. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-71
[38] Renieris E.M., Kiron D., Mills S. Organizations face challenges in timely compliance with the EU AI Act. MIT Sloan Management Review, 13 June 2024. Available at: https://sloanreview.mit.edu/article/organizations-face-challenges-in-timely-compliance-with-the-eu-ai-act/
[39] Buscemi A., Deckenbrunnen T., Kabir F., Mishchenko K., Mowla N. Assessing high-risk AI systems under the EU AI Act: From legal requirements to technical verification. arXiv, 2025. DOI: 10.48550/arXiv.2512.13907
[40] Long D., Magerko B.S. What is AI literacy? Competencies and design considerations. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Article 598, 2020, pp. 1-16. Association for Computing Machinery. DOI: 10.1145/3313831.3376727
[41] GDPRLocal. AI literacy for businesses: What it is and why it matters. 20 June 2025. Available at: https://gdprlocal.com/ai-literacy-for-businesses/

[42] World Economic Forum. Why AI literacy is crucial for responsible AI transformation. 29 July 2025. Available at: https://www.weforum.org/stories/2025/07/ai-literacy-and-strategic-transformation/
[43] Kliemt. Fluent in AI: How to build an AI-literate workforce. Kliemt Blog, 18 September 2025. Available at: https://kliemt.blog/2025/09/19/fluent-in-ai-how-to-build-an-ai-literate-workforce/
[44] Artificial Intelligence Act Service Desk. AI Act Single Information Platform. European Commission, 2024. Available at: https://ai-act-service-desk.ec.europa.eu/en
[45] BearingPoint. The AI Act requires human oversight. BearingPoint, February 2025. Available at: https://www.bearingpoint.com/en-se/insights-events/insights/the-ai-act-requires-human-oversight/
[46] University of South Florida. The role of artificial intelligence in occupational safety and health practices. 20 March 2024. Available at: https://www.usf.edu/health/public-health/news/2024/ai-in-osh-practices.aspx
[47] Dietvorst B.J., Simmons J.P., Massey C. Algorithm aversion: People erroneously avoid algorithms after seeing them err. Journal of Experimental Psychology: General, vol. 144, No 1, 2015, pp. 114-126. DOI: 10.1037/xge0000033
[48] Goddard K., Roudsari A., Wyatt J.C. Automation bias: A systematic review of frequency, effect mediators, and mitigators. Journal of the American Medical Informatics Association, vol. 19, No 1, 2012, pp. 121-127. DOI: 10.1136/amiajnl-2011-000089
[49] Filiz I., Judek J.R., Lorenz M., Spiwoks M. The extent of algorithm aversion in decision-making situations with varying gravity. PLOS ONE, vol. 18, No 2, 2023, e0278751. DOI: 10.1371/journal.pone.0278751
[50] EY ReACT. EU AI Act human oversight requirements: Comprehensive implementation guide. [online] [01.03.2026]. Available at: https://www.eyreact.com/eu-ai-act-human-oversight-requirements-comprehensive-implementation-guide/
[51] Arm. AI today, AI tomorrow: The Arm 2020 global AI survey. Arm, 2020. Available at: https://www.arm.com/resources/report/ai-today-ai-tomorrow
[52] Eslami M., Rickman A., Vaccaro K., Aleyasen A., Vuong A., Karahalios K., Hamilton K., Sandvig C. "I always assumed that I wasn't really that close to (her)": Reasoning about invisible algorithms in news feeds. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15), 2015, pp. 153-162. Association for Computing Machinery. DOI: 10.1145/2702123.2702556
[53] Eslami M., Vaccaro K., Lee M.K., Elazari Bar On A., Gilbert E., Karahalios K. User attitudes towards algorithmic opacity and transparency in online reviewing platforms. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19), Paper 494, 2019. Association for Computing Machinery. DOI: 10.1145/3290605.3300724
[54] Fast E., Horvitz E. Long-term trends in the public perception of artificial intelligence. Proceedings of the AAAI Conference on Artificial Intelligence, vol. 31, No 1, 2017. DOI: 10.1609/aaai.v31i1.10635
[55] Stone P., Brooks R., Brynjolfsson E., Calo R., Etzioni O., Hager G., Hirschberg J., Kalyanakrishnan S., Kamar E., Kraus S., Leyton-Brown K., Parkes D., Press W., Saxenian A., Shah J., Tambe M., Teller A. Artificial intelligence and life in 2030: Report of the 2015-2016 study panel. Stanford University, 2016. Available at: https://ai100.stanford.edu/2016-report
[56] Burrell J. How the machine "thinks": Understanding opacity in machine learning algorithms. Big Data & Society, vol. 3, 2016, pp. 1-12. DOI: 10.1177/2053951715622512
[57] Dubickis M., Zarina A., Putans R. Factors affecting knowledge transfer: A systematic literature review and the method to assess manufacturing company's readiness for knowledge transfer projects. Economics and Culture, vol. 21, No 2, 2024, pp. 1-33. DOI: 10.2478/jec-2024-0016
[58] European Commission. Ethics guidelines for trustworthy AI. European Commission, High-Level Expert Group on Artificial Intelligence, 8 April 2019. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[59] Koutrintzes D., Spatharis C., Dagioglou M. Human-aware design for transferring knowledge during human-AI co-learning. 19 October 2024. Available at: https://manolo-project.eu/wp-content/uploads/2025/03/Camera_Ready_Paper-05.pdf
[60] Amazu C.W. et al. Human-in-the-loop decision support in process control rooms. Data in Brief, vol. 53, 2024, 110170. DOI: 10.1016/j.dib.2024.110170

[61] Risk-First. Human in the loop. Artificial Intelligence Risk Framework. [online] [01.03.2026]. Available at: https://riskfirst.org/ai/Practices/Human-In-The-Loop
[62] European Agency for Safety and Health at Work. Implementing safer AI worker management through policy and prevention. EU-OSHA, 20 April 2025. Available at: https://osha.europa.eu/en/oshnews/implementing-safer-ai-worker-management-through-policy-and-prevention
[63] Baker D.B., Kaye J., Terry S.F. Privacy, fairness, and respect for individuals. eGEMs (Generating Evidence & Methods to Improve Patient Outcomes), vol. 4, No 2, Article 7, 2016. DOI: 10.13063/2327-9214.1207
[64] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. Official Journal of the European Union, 12 July 2024. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
[65] Laux J. Institutionalised distrust and human oversight of artificial intelligence: Towards a democratic design of AI governance under the European Union AI Act. AI & Society, vol. 39, 2024, pp. 2853-2866. DOI: 10.1007/s00146-023-01777-z
[66] Bessaad N., Atsyo S., Hanjie D., Walkine I., Dhillon R., He L. Autonomous mowing in agriculture: Current status, needs, and future opportunities. Smart Agricultural Technology, vol. 13, 2026, 101796. DOI: 10.1016/j.atech.2026.101796
[67] Bowdler M., Lahti H., Jelenko M., Buresti G., Valtonen T. Algorithmic management and psychosocial risks at work: An emerging occupational safety and health challenge. Scandinavian Journal of Work, Environment & Health, vol. 52, No 1, 2026, pp. 1-5. DOI: 10.5271/sjweh.4270
[68] Özkiziltan D., Landini F. Trustworthy and human-centric? The new governance of workplace AI technologies under the EU's Artificial Intelligence Act. Transfer: European Review of Labour and Research, vol. 31, No 4, 2025, pp. 503-517. DOI: 10.1177/10242589251336193
[69] König C.J. Electronic monitoring at work. Annual Review of Organizational Psychology and Organizational Behavior, vol. 12, 2025, pp. 321-342. DOI: 10.1146/annurev-orgpsych-110622-060758
[70] Kayas O.G. Workplace surveillance: A systematic review, integrative framework, and research agenda. Journal of Business Research, vol. 168, 2023, 114212. DOI: 10.1016/j.jbusres.2023.114212
[71] Siegel R., König C.J., Lazar V. The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. Computers in Human Behavior Reports, vol. 8, 2022, 100227. DOI: 10.1016/j.chbr.2022.100227
[72] Feeser V.R., Jackson A.K., Savage N.M., Layng T.A., Senn R.K., Dhindsa H.S., Santen S.A., Hemphill R.R. When safety event reporting is seen as punitive: "I've been PSN-ed!" Annals of Emergency Medicine, vol. 77, No 4, 2021, pp. 449-458. DOI: 10.1016/j.annemergmed.2020.06.048
[73] Glavin P., Bierman A., Schieman S. Private eyes, they see your every move: Workplace surveillance and worker well-being. Social Currents, vol. 11, No 4, 2024, pp. 327-345. DOI: 10.1177/23294965241228874
[74] EU AI Risk Team. Human oversight requirements: Balancing automation with accountability. EU AI Risk. [online] [01.03.2026]. Available at: https://euairisk.com/resources/human-oversight-balancing-automation-accountability
[75] European Commission. AI literacy - Questions & answers. Shaping Europe's digital future. [online] [01.03.2026]. Available at: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
[76] European Data Protection Supervisor. TechDispatch 2/2025: Human oversight of automated decision-making. 23 September 2025. Available at: https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-09-23-techdispatch-22025-human-oversight-automated-making_en
[77] European Commission. Requirements for trustworthy AI. FUTURIUM. [online] [01.03.2026]. Available at: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html

[78] Nilsson K.H., Matilla-Santander N., Lee M.K., Brulin E., Bodin T., Håkansta C. Algorithmic management and occupational health: A comparative case study of organizational practices in logistics. Safety Science, vol. 187, 2025, 106863. DOI: 10.1016/j.ssci.2025.106863
[79] Havinga J., Bancroft K., Rae A. Deciding to stop work or deciding how work is done? Safety Science, vol. 141, 2021, 105334. DOI: 10.1016/j.ssci.2021.105334
[80] Chen R.R., Gao J., Chen X., Huang Q. Blessing or curse? The two-sided effects of algorithmic control on ego-depletion and safety performance of gig workers. Computers in Human Behavior, vol. 162, 2025, 108461. DOI: 10.1016/j.chb.2024.108461
[81] Palmiotto F. The AI Act roller coaster: The evolution of fundamental rights protection in the legislative process and the future of the regulation. European Journal of Risk Regulation, vol. 16, No 2, 2025, pp. 770-793. DOI: 10.1017/err.2024.97

Annex 1. Research Survey Questions.

List of survey questions. (Survey link (questionnaire) is available also at Lime survey platform – https://limesurvey.ttu.ee/limesurvey/index.php/747791)

Q1-Q7. Socio-demographic questions: Q1.Age; Q2.Sex; Q3.Country; Q4.Profession or field of activity; Q5.Job role or function; Q6.Industry sector; Q7.Company size.

Q8. High-risk AI system usage. Q8. Please indicate if your company uses AI for the following tasks.

Q8.1.AI systems for biometric identification (e.g., facial recognition)
Q8.2.AI systems for biometric categorization based on sensitive attributes (e.g., sex, race)
Q8.3.AI systems intended for emotion recognition.
Q8.4.AI systems for evaluating learning outcomes.
Q8.5.AI systems for assessing appropriate education levels.
Q8.6.AI systems for monitoring and detecting prohibited behaviors during tests.
Q8.7.AI systems for recruitment and selection processes.
Q8.8.AI systems for making decisions affecting work-related terms.
Q8.9.AI systems for promotion and termination of employment.
Q8.10.AI systems for task allocation based on individual behavior or personal characteristics.
Q8.11.AI systems for monitoring or evaluation of employees.
Q8.12.AI systems for evaluating the creditworthiness or credit scoring of individuals.
Q8.13.AI systems for risk assessment and pricing in life and health insurance.
Q8.14.AI systems for Supply Chain Optimization.
Q8.15.AI systems for Predictive Maintenance.

Q9. Non high-risk AI system usage. Q9. Please indicate if your company uses AI for the following tasks.

Q9.1.AI systems for Marketing
Q9.2.AI systems for Sales
Q9.3.AI systems for Customer relationships
Q9.4.AI systems for Customer service
Q9.5.AI systems for Human resources
Q9.6.AI systems for Employee training
Q9.7.AI systems for Finance
Q9.8.AI systems for Supply chain & Logistics
Q9.9.AI systems for Operations
Q9.10.AI systems for Product and service development
Q9.11.AI systems for Business intelligence & analytics
Q9.12.AI systems for Health and safety
Q9.13.AI systems for Legal management
Q9.14.AI systems for Property management
Q9.15.AI systems for Cybersecurity
Q9.16.AI systems for Communication

Q10. AI Literacy. Assess how much the following statements apply to your organisation. Please respond to each statement by selecting a number from 1 to 5, where: 1 = Not all. 2 = 0. 3 = 0. 4 = 0. 5 = Very much.

Q10.1. Our company has taken sufficient measures to ensure that employees in key roles possess adequate AI literacy.
Q10.2. Our company actively prioritizes developing technical knowledge and offering training for AI system operations.
Q10.3. Our company is well-informed about potential harm or risks associated with AI systems.

Q11. Human oversight of AI. Assess how much the following statements apply to your organisation. Please respond to each statement by selecting a number from 1 to 5, where: 1 = Not all, 5 = Very much.

Q11.1. Individuals responsible for overseeing high-risk AI systems within our company possess the necessary competence.
Q11.2. Individuals assigned to oversee high-risk AI systems in our organization have sufficient authority to perform oversight effectively.
Q11.3. Our company consistently provides training and resources for employees tasked with overseeing high-risk AI systems.

Q12. Monitoring and Reporting. Assess how much the following statements apply to your organisation. Please respond to each statement by selecting a number from 1 to 5, where: 1 = Not all, 5 = Very much.

Q.12.1. Our company implements the necessary technical and organizational measures to ensure the proper use of AI systems
Q.12.2. Our company regularly monitors the performance and outcomes of high-risk AI systems.
Q12.3. When issues arise with AI systems, our company promptly reports them to the relevant authorities.

Q13. Data Relevance and Representativeness. Assess how much the following statements apply to your organisation. Please respond to each statement by selecting a number from 1 to 5, where: 1 = Not all, 5 = Very much.

Q13.1. Our company ensures that the input data is highly relevant to the purpose of the high-risk AI system.

Q13.2. The input data used by our company is sufficiently representative of the intended purpose or population for the high-risk AI system.

Q14. Transparency and Communication. Assess how much the following statements apply to your organisation. Please respond to each statement by selecting a number from 1 to 5, where: 1 = Not all, 5 = Very much.

Q14.1. Our company communicates proactively with workers' representatives regarding the use of high-risk AI systems.

Q14.2. Our company informs individual workers directly when high-risk AI systems could affect them.

Q14.3. Individuals are adequately informed when decisions impacting them are made using high-risk AI systems.

Q15. Fundamental Rights Impact Assessment. Assess how much the following statements apply to your organisation. Please respond to each statement by selecting a number from 1 to 5, where: 1 = Not all, 5 = Very much.

Q15.1. Our company conducts thorough impact assessments on fundamental rights prior to deploying high-risk AI systems.

Q15.2. Our company identifies potential risks to individuals' rights associated with high-risk AI systems.

Q15.3. Our company has clear measures in place to mitigate these risks if they occur.

Q16. Registration

Q16.1. Our company considers registering high-risk AI systems with the relevant public authorities (where applicable)

Q16.2. Our company avoids using any unregistered high-risk AI systems.

Q16.3. If a high-risk AI system is unregistered, our company takes steps to inform the provider or distributor.

Q17. What challenges have you faced regarding human-AI interaction at your workplace? Open-ended question.

Q18. What improvements can be made at your work to make AI human-centered? Open-ended question.