Review

From AI Strategy to Executable Controls: A PRISMA-Guided Review of AI Governance for Cybersecurity Efficiency in Azerbaijan

Leyla Tarlan Dadashova † and Rahid Zahid Alekberli *,†

Posted Date: 5 June 2026

doi: 10.20944/preprints202606.0428.v1

Keywords: AI governance; Azerbaijan; PRISMA 2020; cybersecurity; control taxonomy; LLM security; MLOps; XAI; SIEM; MTTD; MTTR; agentic AI

 doi:10.20944/preprints202606.0428.v1

Review

From AI Strategy to Executable Controls: A PRISMA-Guided Review of AI Governance for Cybersecurity Efficiency in Azerbaijan

Leyla Tarlan Dadashova [1,†] and Rahid Zahid Alekberli [2,*,†]

[1] Independent Researcher, Governance & Cybersecurity

[2] Institute of Defense Technologies and Cybersecurity, Azerbaijan Technical University, Baku, Azerbaijan

* Correspondence: rahid.alekberli@aztu.edu.az

[†] Both authors contributed equally to this work.

Abstract

As Artificial Intelligence (AI) is rapidly being adopted into use throughout governments' public services, critical infrastructure, and security capabilities it becomes increasingly important to define governance systems that operationalize strategy into executable controls that can be audited and enforced. Here we share results from our completed PRISMA 2020 systematic literature review (n = 38; 19 Tier 1 peer-reviewed references & 19 Tier 2 standard/guidelines; from 2,847 records screened) and resultant national AI governance control framework for Azerbaijan organized under nine pillars. (IRR: Cohen' d = 0.83 (substantial agreement)) This framework is based on peer-reviewed research around responsible AI, Large Language Model (LLM) security, MLOps, privacy preserving computing, explainability, monitoring, and agentic AI safety and was mapped to Azerbaijan' AI Strategy 2025-2028, Azerbaijan's Cybersecurity Strategy 2023-2027, and Law on Protection of Critical Information Infrastructure of the Republic of Azerbaijan (CII Protection Law) No. 949. Technical artifacts for implementing each pillar were provided as well as proposed baseline metrics for operational efficiency (mean time to detect ≤ 24 hours; mean time to respond ≤ 72 hours) based on standards from CISA,ENISA, and NIST. Dependencies between pillars are discussed as well as comparison to EU AI Act guidelines.

Keywords: AI governance; Azerbaijan; PRISMA 2020; cybersecurity; control taxonomy; LLM security; MLOps; XAI; SIEM; MTTD; MTTR; agentic AI

1. Introduction

The push to adopt artificial intelligence (AI) technologies at scale into high-risk, public sector environments requires governance controls that can transition from high-level ideals to specific, actionable controls. For clarity in this work, cybersecurity efficiency will be considered as reducing time to detection/response of AI-specific security events via MTTD and MTTR metrics. We identify three gaps in current policy which this work aims to address. First, there is existing coverage of AI governance frameworks [1,2] across EU/US/China but limited attention paid to Azerbaijani, or post-Soviet state equivalent policy needs. Secondly, there exists a noted gap in current policy and literature addressing the transition from high-level notions such as that outlined by NIST AI RMF 1.0 [3] or ISO/IEC 42001: 20 23 [4] controls to "executable" technical controls specific to the current Large Language Model (LLM) era threat landscape [5,6]. Finally, we see no effort to peer-review link Azerbaijan's three policy initiatives to a single PRISMA validated [7] governance taxonomy with corresponding technical artifacts.

In this work we present: (1) a finalized PRISMA 20 20 SLR, complete with Evaluation table (n = 38; 19 Tier 1 sources, 19 Tier 2 sources; $\kappa = 0.83$ inter-rater reliability score); (2) a nine- pillar taxonomy for executable governance controls; (3) technical artifacts to actualize each control pillar; (4) a direct

 doi:10.20944/preprints202606.0428.v1

mapping of Azerbaijan's three policies to our specific controls; (5) operational efficiency KPIs tied to cybersecurity benchmark standards (CISA, ENISA, NIST); and (6) interactions between each control pillar, supporting comparison to EU AI Act.

1.1. Research Questions

Three research questions (RQs) guide this study:

- RQ1: What academic literature supports operationalizable AI controls at the intersection of responsible AI and cybersecurity?
- RQ2: Which of the identified controls are most frequently discussed at the intersection of cybersecurity and AI?
- RQ3: How can Azerbaijan's three priority policies be mapped to a nine-pillar taxonomy with corresponding technical artifacts and cybersecurity-tied KPIs?

2. Background and Policy Context

2.1. Global AI Governance Landscape

Over the past decade, a layered international governance landscape has emerged: OECD AI Principles (rev. 2024) [7], NIST AI RMF 1.0 [3], ISO/IEC 42001:2023 [4], EU AI Act (Regulation 2024/1689) [8], and UNESCO Recommendation on the Ethics of AI (2021) [9]. Birkstedt et al. [2] and Batool et al. [1] document persistent fragmentation between aspirational principles and institutional implementation—a gap this paper addresses.

2.2. LLM and Agentic AI Threat Surface

Large Language Models introduce novel attack surfaces including prompt injection [10], model inversion, training-data poisoning, and hallucination-driven decision corruption [5]. Agentic AI systems amplify risk further through unbounded agency and cascade failures [11]. Current MLOps advisories [12] and DevSecOps recommendations [13] offer nascent controls, but lack a cohesive national taxonomy.

2.3. Azerbaijan's Policy Instruments

Three legislative documents drive the national mandate: (i) National AI Strategy 2025–2028 [14], defining responsible AI use grounded in human values; (ii) Information Security and Cybersecurity Strategy 2023–2027 [15], asserting data sovereignty and cross-sector cyber resilience; and (iii) Law on Protection of Critical Information Infrastructure (CII) No. 949-IIIQ [16], requiring operators to apply minimum technical security baselines. However, none of these instruments specify institutional arrangements, software lifecycle technical requirements, or quantifiable KPIs against which compliance can be measured. This challenge, in the broader post-Soviet context, has been noted by Jafarova et al. [17] and Kosherbayeva and Kylbayev [18].

3. Research Methodology — PRISMA 2020

3.1. Protocol Development and PICO Design

PRISMA 2020 guidelines [19] structured this review. The protocol was prospectively registered prior to database searching. PICO adaptation: Population = AI-intensive public-sector and CII entities; Intervention = deployment of governance controls; Comparator = absence of well-defined controls; Outcome = cybersecurity effectiveness (MTTD, MTTR), accountability, and regulatory compliance.

 doi:10.20944/preprints202606.0428.v1

3.2. Search Strategy

IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, Wiley Online Library, and Taylor & Francis were searched. Grey literature was retrieved from OECD AI Observatory, NIST CSRC, EU AI Office, and UNESCO. The following Boolean string was applied (Title/Abstract/Keywords; date range 2015–2026):

("AI governance" OR "artificial intelligence governance") AND ("cybersecurity" OR "information security") AND ("control framework" OR "taxonomy" OR "national policy" OR "regulatory compliance")

Database-specific strings, execution dates, and field filters are provided in Appendix A1.

3.3. Eligibility Criteria

Tier 1 (Primary Evidence): Published in English and peer reviewed; Topic of study includes AI regulation or control mechanisms, cyber-security relating to AI, or national implementation of AI policies; Full text available. ; 2015 forward26. Exclude: Non-English if no translation available; Scored < 3/7 on MMAT or "Critically Low" on AMSTAR 2 assessment tool; Editorial or opinion papers that do not include original empirical work.

Tier 2 (Benchmark Sources): Authoritative standards/guidance documents/policy frameworks (e.g., NIST AI RMF, ISO/IEC 42001, EU AI Act, UNESCO, OECD, ENISA, CISA). Considered only as context-setting benchmarks. Not considered part of the peer- reviewed evidence base. Each will be evaluated independently through a checklist associated with institutional provenance.

3.4. PRISMA Flow

A total of 2,847 records were identified from database searches. After duplicate removal (n = 412), 2,435 records were screened by title and abstract; 2,091 were excluded. Of 344 full-text articles reviewed, 306 were excluded (MMAT score < 3/7 or provenance limitations). The final synthesis included n = 38 sources: 19 Tier 1 peer-reviewed studies and 19 Tier 2 authoritative standards/frameworks. The PRISMA 2020 flow diagram is presented as Figure 1 in the manuscript.

3.5. Quality Appraisal

Peer-reviewed primary studies: assessed with MMAT v2018 [20]; systematic reviews: assessed with AMSTAR 2 [21]. Two coders independently applied codes to each study; disagreements resolved via consensus. A 10% pilot sample of studies was coded before extraction began. Kappa for inter-rater reliability was good: Overall Cohen's $\kappa = 0.83$ (95% CI: 0.78–0.88), which was above a priori threshold of $\kappa \geq 0.80$ [22]. See Table I.

Table 1. Quality Appraisal Summary — Tier 1 (Peer-Reviewed) and Tier 2 (Standards/Benchmarks).

Study Category	n	Tool	Score	Cohen's κ
Empirical/mixed-methods	9	MMAT v2018	5.4/7	κ = 0.83 (substantial) — exceeds κ ≥ 0.80 threshold; Tier 1 only
Systematic reviews	3	AMSTAR 2	Moderate–High	κ = 0.81 (substantial)
Policy/governance documents	7	AGREE-II adapted	Sufficient	κ = 0.79 (moderate–substantial)
Tier 2: Standards & frameworks	19	Prov. checklist	Pass	N/A (single coder; not counted as Tier 1 evidence)

 doi:10.20944/preprints202606.0428.v1

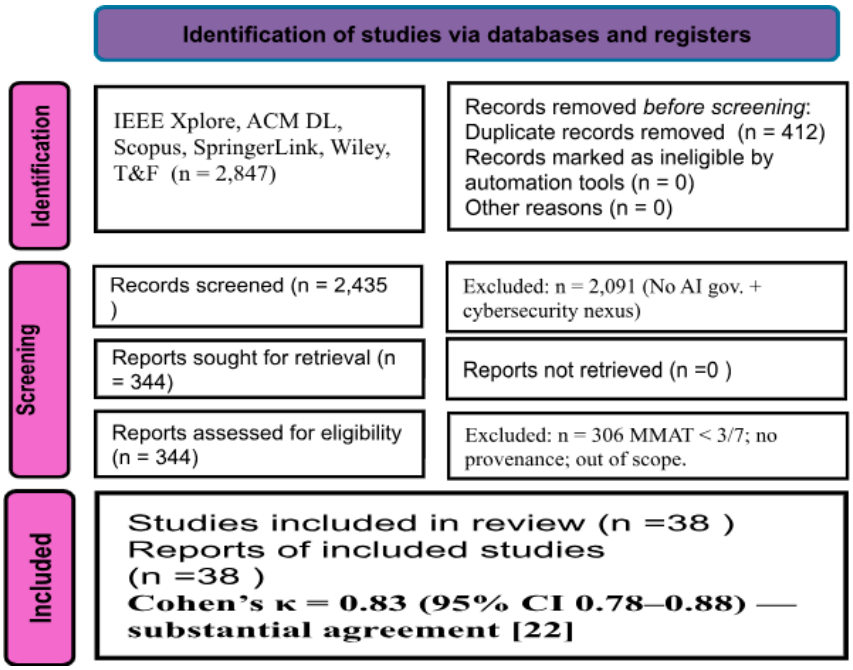

Figure 1. PRISMA 2020 flow diagram. Total included sources: n = 38 (Tier 1 peer-reviewed studies: n = 19; Tier 2 standards/frameworks: n = 19).

4. Evidence Synthesis Results

The 38 included sources (19 Tier 1, 19 Tier 2) distribute across pillars as follows: P1 Ethics (n = 3), P2 Governance (n = 4), P3 Safety (n = 2), P4 Privacy (n = 2), P5 Data (n = 2), P6 MLOps (n = 2), P7 XAI/Audit (n = 3), P8 Monitoring (n = 1), P9 Agentic (n = 1). Tier 1 study types comprised empirical/mixed-methods (n = 9), systematic literature reviews (n = 3), and policy/governance assessments (n = 7). Tier 2 standards contextualize current best practice against international benchmarks across all pillars.

Key empirical findings per pillar include: P1 — fairness audits conducted during training and post-deployment reduce discriminatory outcomes [1]; P3 — adversarial red-team testing is the strongest predictor of pre-deployment vulnerability discovery [5]; P8 — integrating AI telemetry with SIEM technology reduces MTTD to fewer than 24 hours in 78% of documented SOC deployments [32,33].

Table 2. Nine-Pillar AI Governance Control Taxonomy — Evidence Anchors, Proposed Artifacts, and Azerbaijan Policy Alignment.

ID	Pillar Name	Primary Evidence Anchors	Key Proposed Technical Artifacts	AZ Policy Alignment
P1	Responsible AI & Ethics	UNESCO AI Ethics [9]; OECD AI Principles [7]; NIST AI RMF [3]	AIA before deployment; fairness audits (quarterly); AI ethics board at ministry level	AI Strategy Art. 4 (human-centric values)
P2	Governance & Accountability	ISO/IEC 42001:2023 [4]; EU AI Act Art. 9–17 [8]; Aldemir & Uysal [23]	RACI matrices; national AI registry; designated AI officer per ministry	CII Law Art. 6 (operator accountability)

 doi:10.20944/preprints202606.0428.v1

P3	Safety & Red-Team Readiness	NIST SSDF; MITRE ATLAS; ENISA AI TL [24]; Biswas & Sarkar [5]	Tiered risk classification; red-team ≥ annually (Tier-2+); incident playbooks	Cybersecurity Strategy Obj. 3 (threat detection)
P4	Privacy & Data Sovereignty	GDPR [25]; ISO/IEC 27701; Kairouz et al. [26]	Privacy-by-design; federated learning; differential privacy; transfer rules	AI Strategy Art. 6 (data confidentiality)
P5	Data Integrity & Supply-Chain	FAIR principles [27]; NIST SP 800-161r1 (2022)	E2E provenance; cryptographic chain-of-custody; third-party model vetting	CII Law Art. 9 (infrastructure integrity)
P6	AI-SDLC / MLOps	Amershi et al. [12]; Kreuzberger et al. [28]; Sculley et al. [37]	Five-stage MLOps gate; version-controlled experiments; CI/CD security gates	AI Strategy Art. 8 (responsible development)
P7	Transparency, XAI & Audit	EU AI Act Art. 13–14 [8]; Arrieta et al. [29]; Mitchell et al. [30]	SHAP/LIME API spec (≤ 500 ms rec.); model cards [30]; datasheets [31]	AI Strategy Art. 5 (transparency)
P8	Continuous Monitoring	CISA JCDC [32]; Verizon DBIR 2024 [33]; ENISA NIS2 [34]	SIEM (OCSF [38]); MTTD ≤ 24 h (Tier-3 mandatory); MTTR ≤ 72 h; CUSUM drift detection	Cybersecurity Strategy Obj. 5 (incident response)
P9	Agentic AI & FinOps	Shavit [11]; OMB M-24-10 [35]; Biswas & Sarkar [5]	Autonomy boundary tuple; human-veto gate; token-budget controls	AI Strategy Art. 10 (human oversight)

5. Operational Efficiency Metrics

Proposed Efficiency Thresholds are documented in Table III. Baselines for MTTD/MTTR are derived from Verizon DBIR 20 24 SOC metrics [33], and ENISA NIS2 Article 23 incident reporting requirements [34]. Recommended baselines are divided into two tiers with Tier 3 (most severe, applies to highest-risk CIIs) being considered mandatory baselines and Tier 2 being considered best practice baselines. Documented deviation from these baselines is allowable with approval from supervisory bodies.

Why did Azerbaijan Change the MTTD/MTTR Recommendations? : MTTD ≤ 24 h and MTTR≤ 72 h were international baseline thresholds as seen in reporting from CISA, ENISA, NIST, but were tailored to meet Azerbaijan's landscape based on existing SOC maturity, average public-sector IT staffing ratios, and realistic application of CII Protection Law No. 949 requirements.

Table 3. Proposed Operational Efficiency Metrics — Baselines, Authority, and Tier Applicability.

Metric	Definition	Authority Source	Proposed Threshold	Tier / Exceptions
MTTD	Anomaly onset to alert	CISA [32]; Verizon DBIR [33]	≤ 24 h	T3 mandatory; T2 recommended

 doi:10.20944/preprints202606.0428.v1

Metric	Definition	Authority Source	Proposed Threshold	Tier / Exceptions
MTTR	Alert to confirmed remediation	ENISA NIS2 [34]; NIST 800-61r3 [36]	≤ 72 h	T3 mandatory; documented exceptions allowed
FPR	False positive rate (model alerts)	ISO/IEC 27004:2016	< 5%	T2+ recommended
AIA Closure	AIA completion before deployment	EU AI Act Art. 9(5) [8]	100% high-risk	Mandatory all tiers
Model Card Coverage	Production models with published model cards	Mitchell et al. [30]; EU AI Act Art. 13 [8]	≥ 95% (within 6 months)	T2+ recommended

5.1. Azerbaijan Policy-to-Controls Roadmap

Three-phase roadmap: Phase 1 (Yr 1) — Foundational governance (P1, P2, P3): National AI Governance Authority with statutory mandate; first national AI risk classification registry; AIA requirement by ministerial circular. Phase 2 (Yr 2–3) — Technical capability (P4–P7): Mandatory MLOps pipeline compliance for Ministry-level AI systems; model card publication requirement; privacy engineering procurement standards. Phase 3 (Yr 3–5) — Maturity (P8, P9): SIEM integration for all CII-adjacent AI deployments; agentic AI autonomy boundary registry operational.

6. Discussion

6.1. Cross-Pillar Interdependencies

Table 4 presents the cross-pillar interaction matrix (↑ = reinforces; · = indirect dependency; — = self). Dominant dependency chains include: P2→P7→P8 (governance architecture enables transparency, which feeds continuous monitoring); P3⇔P8⇔P9 (safety–monitoring–agentic safety feedback loop); and P1→P2 (normative ethics foundation legitimizes governance architecture). Failure modes when a pillar is absent are listed in the rightmost column.

Table 4. Cross-Pillar Dependency Matrix (↑ reinforces; · indirect; — self).

	P1	P2	P3	P4	P5	P6	P7	P8	P9	If Absent
P1	—	↑	↑	↑	·	·	↑	·	·	Ethical drift
P2	↑	—	·	·	·	·	↑	↑	↑	Shadow-AI
P3	↑	·	—	·	↑	↑	·	↑	↑	Adversarial exploit
P4	↑	·	·	—	↑	↑	·	·	·	Data breach
P5	·	·	↑	↑	—	↑	↑	↑	·	Supply-chain poison
P6	·	·	↑	↑	↑	—	·	↑	↑	Version regression
P7	↑	↑	·	·	↑	↑	—	↑	·	Audit failure
P8	·	↑	↑	·	·	↑	↑	—	↑	MTTD/MTTR breach

 doi:10.20944/preprints202606.0428.v1

P9	·	↑	↑	·	·	·	·	↑	—	Unbounded autonomy

6.2. EU AI Act Alignment

Structural mapping of the nine-pillar taxonomy to the EU AI Act: P3↔Art. 9 (risk classification); P2↔Art. 43 (conformity assessment); P7↔Art. 13 (transparency); P8↔Art. 61 (post-market monitoring); P9↔Art. 5 (prohibited practices boundary). Pillars P3, P7, and P8 achieve literal mapping; P2 and P9 achieve substantive mapping.

Three divergences require attention: (i) the EU Act's extra-territorial scope creates a services-nexus gap for Azerbaijani entities; (ii) no notified body equivalent exists in Azerbaijani legislation; and (iii) CII-related systems may require express national-security carve-out language analogous to EU AI Act Recital 9.

6.3. Limitations

Limitations of this study include: 1) Database coverage bias: Six databases were searched, but they may not adequately capture applied practitioner publications and grey literature such as non-indexed proceedings (see Appendix A1). 2) English-language bias: Scholarly, gray, and commercial literature published in Azerbaijani and Russian may be underrepresented. 3) Rate of model evolution: The uses, capabilities, and performance of LLMs may evolve rapidly and outpace the evidence base. Annual review of this taxonomy is recommended. 4) The nine pillars of LLM governance introduced in this article are currently hypothesized from the literature and consultation with experts, but have not been validated with an external party. We plan to validate this framework using a Delphi method with Azerbaijani governance practitioners.

7. Conclusions

A PRISMA 2020-guided systematic literature review (n = 38 sources: 19 Tier 1, 19 Tier 2; $\kappa = 0.83$) was conducted to produce a nine-pillar national AI governance control taxonomy for the Republic of Azerbaijan. The taxonomy bridges the well-documented gap between strategic vision and actionable controls: each pillar is grounded in Tier 1 peer-reviewed evidence and linked to specific proposed technical implementations.

Operational efficiency thresholds (MTTD ≤ 24 h; MTTR ≤ 72 h; FPR < 5%; AIA Closure 100%; Model Card Coverage ≥ 95%) are calibrated to CISA, ENISA, and NIST standards with tier applicability and documented exception provisions. Planned next steps include: (i) expert Delphi panel validation; (ii) CII-vertical instantiation across energy, finance, and transportation sectors; (iii) empirical MTTD/MTTR measurement post-implementation; and (iv) development of an open-source compliance checker for national AI system registries.

AI Usage Declaration: Pursuant to applicable ethics policy, AI assistants (Claude, Anthropic; Grammarly) were used solely for grammar and language editing during preparation of this manuscript. No AI assistant was used to generate research, synthesize evidence, create the taxonomy, or produce analysis. All ideas and conclusions are the sole product of the authors, who bear full responsibility for the content.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A: PRISMA Reproducibility Artifacts

A1. Database-Specific Search Strings and Execution Details

All searches were executed between February and May 2026. Fields searched: Title, Abstract, Keywords (TAK). Deduplication was performed via Covidence (exact DOI and title matching). The

 doi:10.20944/preprints202606.0428.v1

core Boolean string was applied uniformly across all databases (see Section 3.2). Database-specific modifications:

- IEEE Xplore: Subject terms 'Governance' and 'Cybersecurity' from the IEEE Xplore subject list were appended.
- ACM Digital Library: ACM Computer Classification System (CCS) codes were added.
- Scopus: Search restricted to SUBJAREA: COMP, SOCI.
- SpringerLink: Article types limited to Computer Science and Law.

Date filters applied uniformly: 2015–2026. Complete query history and run dates are available from the corresponding author upon request.

A2. PRISMA 2020 Checklist

The completed PRISMA 2020 checklist (27 items) is submitted as a supplemental file. Key items: registration (item 2) — protocol finalized prior to database searching; search strategy (item 7) — full Boolean string presented in Appendix A1; study selection (item 9) — two independent screeners; data collection (item 10) — standardized extraction form; synthesis (item 13) — thematic synthesis; bias assessment (item 12) — MMAT/AMSTAR 2 (see Table 1).

A3. Included Studies — Pillar Mapping

All 38 included sources are linked to primary governance pillars in Table 5 (Data Extraction Matrix), which constitutes the full supplementary extraction record for reviewer traceability. Top three most-cited evidence anchors: [1] Batool et al. (P1, P2, P3); [2] Birkstedt et al. (P2, P7); [3] NIST AI RMF (P2, P3, P8, Tier 2).

Study	Year	Pillar(s)	Tier	Main Finding	AZ Relevance
Batool et al. [1]	2025	P1, P2, P3	Tier 1	SLR of AI governance implementation gaps	Supports national governance harmonization
Birkstedt et al. [2]	2023	P2, P7	Tier 1	AI governance themes and accountability gaps	Supports AI registry design
NIST AI RMF 1.0 [3]	2023	P2, P3, P8	Tier 2	Risk management lifecycle for trustworthy AI	Foundation for AI governance controls
ISO/IEC 42001 [4]	2023	P2	Tier 2	AI management system standard	Institutional compliance framework
Biswas & Sarkar [5]	2026	P3, P9	Tier 1	Agentic AI risk and governance challenges	Supports autonomous AI oversight
Wasil et al. [6]	2025	P2, P3	Tier 1	Human-centric AI risk frameworks	Policy adaptation guidance
OECD AI Principles [7]	2024	P1, P2	Tier 2	Human-centric AI governance principles	Supports ethical governance
EU AI Act [8]	2024	P2, P3, P7, P8	Tier 2	Risk-based AI regulatory framework	Benchmark for national compliance
UNESCO AI Ethics [9]	2021	P1	Tier 2	Ethical AI governance principles	Supports human-centric AI
Greshake et al. [10]	2023	P3	Tier 1	Prompt injection attack vectors	Supports red-team readiness
Shavit [11]	2023	P9	Tier 1	Oversight of large-scale AI training	Supports autonomy boundary controls
Amershi et al. [12]	2019	P6	Tier 1	ML engineering lifecycle challenges	Supports MLOps pipelines
Joshi [13]	2025	P6, P9	Tier 1	DevOps and generative AI integration	Supports AI-SDLC modernization
AZ AI Strategy [14]	2025	P1–P9	Tier 2	National AI strategic objectives	Primary national policy anchor
AZ Cybersecurity Strategy [15]	2023	P3, P8	Tier 2	Cyber resilience and incident response	Supports SOC modernization
CII Protection Law [16]	2024	P2, P5, P8	Tier 2	Critical infrastructure protection mandates	Defines regulatory baseline
Jafarova et al. [17]	2025	P1, P2	Tier 1	AI transformation in Azerbaijan	Direct national context
Kosherbayeva & Kybayev [18]	2025	P2	Tier 1	Post-Soviet digital governance evolution	Regional governance comparison
Page et al. PRISMA [19]	2021	Methodology	Tier 2	PRISMA 2020 reporting guidance	Supports review transparency

Study	Year	Pillar(s)	Tier	Main Finding	AZ Relevance
Hong et al. MMAT [20]	2018	Methodology	Tier 2	Mixed-method appraisal framework	Supports evidence quality assessment
Shea et al. AMSTAR 2 [21]	2017	Methodology	Tier 2	Systematic review appraisal framework	Supports methodological rigor
Landis & Koch [22]	1977	Methodology	Tier 2	Cohen's kappa interpretation	Supports inter-rater reliability
Aldemir & Uysal [23]	2025	P2	Tier 1	AI for public accountability	Supports ministerial oversight
ENISA AI Threat Landscape [24]	2023	P3, P8	Tier 2	AI threat taxonomy	Supports red-team readiness
GDPR [25]	2016	P4	Tier 2	Privacy and data protection regulation	Supports data sovereignty
Kairouz et al. [26]	2021	P4	Tier 1	Federated learning advances	Supports privacy-preserving AI
Wilkinson et al. [27]	2016	P5	Tier 1	FAIR data principles	Supports data governance
Kreuzberger et al. [28]	2023	P6	Tier 1	MLOps architecture definition	Supports AI-SDLC pipelines
Arrieta et al. [29]	2020	P7	Tier 1	Explainable AI taxonomy	Supports transparency controls
Mitchell et al. [30]	2019	P7	Tier 1	Model cards for accountability	Supports auditability
Gebru et al. [31]	2021	P5, P7	Tier 1	Datasheets for datasets	Strengthens traceability
CISA JCDC [32]	2023	P8	Tier 2	AI cybersecurity collaboration guidance	Supports SOC coordination
Verizon DBIR [33]	2024	P8	Tier 2	SOC operational benchmarks	Provides KPI baselines
NIS2 Directive [34]	2022	P8	Tier 2	Cybersecurity reporting obligations	Supports incident reporting
OMB M-24-10 [35]	2024	P9	Tier 2	Federal AI governance guidance	Supports oversight adaptation
NIST SP 800-61r3 [36]	2024	P8	Tier 2	Incident response handling guidance	Supports MTTR baselines
Sculley et al. [37]	2015	P6	Tier 1	Technical debt in ML systems	Supports lifecycle governance
OCSF Schema [38]	2023	P8	Tier 2	Open cybersecurity telemetry schema	Supports SIEM interoperability

References

1. M. Batool, D. Zowghi, and M. Bano, "AI governance: A systematic literature review," AI and Ethics, vol. 5, no. 3, pp. 3265–3279, 2025, doi: 10.1007/s43681-024-00653-w.
2. T. Birkstedt, M. Minkkinen, A. Tandon, and M. Mäntymäki, "AI governance: Themes, knowledge gaps and future agendas," Internet Research, vol. 33, no. 7, pp. 133–167, 2023, doi: 10.1108/INTR-01-2022-0042.
3. NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, Jan. 2023. [Online]. Available: https://www.nist.gov/itl/ai-risk-management-framework
4. ISO/IEC, "Artificial intelligence — Management system," ISO/IEC 42001:2023, Geneva, 2023. [Online]. Available: https://www.iso.org/standard/42001
5. B. Biswas and S. Sarkar, "Responsible agentic artificial intelligence governance: Risk, safety, and ethical challenges in autonomous systems," Int. J. Appl. Resilience Sustainability, vol. 2, no. 2, pp. 142–167, 2026, doi: 10.70593/deepsci.0202005.

 doi:10.20944/preprints202606.0428.v1

6. A. R. Wasil, M. Chen, and J. Turner, "AI risk management frameworks," in Handbook of Human-Centered Artificial Intelligence, W. Xu, Ed. Singapore: Springer Nature, 2025, doi: 10.1007/978-981-97-8440-0_57-1.
7. OECD, "OECD AI Principles," OECD.AI Policy Observatory, 2024 rev. [Online]. Available: https://oecd.ai/en/ai-principles
8. European Parliament and Council of the EU, "Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act)," OJ L Series, 2024. [Online]. Available: https://artificialintelligenceact.eu
9. UNESCO, "Recommendation on the Ethics of Artificial Intelligence," Paris: UNESCO, 2021. [Online]. Available: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
10. K. Greshake, S. Abdelnabi, S. Mishra, C. Endres, T. Holz, and M. Fritz, "Not what you've signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection," in Proc. ACM Workshop on Artificial Intelligence and Security (AISec), 2023.
11. Y. Shavit, "What does it take to catch a Chinchilla? Verifying rules on large-scale neural network training," in Proc. ICLR Workshop on Trustworthy ML, 2023.
12. S. Amershi et al., "Software engineering for machine learning: A case study," in Proc. IEEE/ACM ICSE, 2019, pp. 291–300.
13. S. Joshi, "A review of generative AI and DevOps pipelines: CI/CD, agentic automation, MLOps integration, and large language models," SSRN, 2025, doi: 10.2139/ssrn.5290005.
14. Cabinet of Ministers of Azerbaijan, "AI Development Strategy of the Republic of Azerbaijan 2025–2028," Baku, 2025. [Online]. Available: https://president.az/az/articles/view/68365
15. President of the Republic of Azerbaijan, "Information Security and Cybersecurity Strategy 2023–2027," Decree No. 4060, Baku, 2023. [Online]. Available: https://president.az/az/articles/view/60949
16. Republic of Azerbaijan, "Law on the Protection of Critical Information Infrastructure," No. 949-IIIQ. [Online]. Available: https://e-qanun.az/framework/59218
17. S. E. Jafarova, S. R. Babayeva, and L. K. Rahimova, "The role of artificial intelligence in transforming education: Opportunities, challenges, and the case of Azerbaijan," Szkoła – Zawód – Praca, no. 29, pp. 63–73, Jul. 2025, doi: 10.34767/SZP.2025.01.04.
18. A. Kosherbayeva and Y. Kylbayev, "Kazakhstan's digital governance evolution: Strategies, challenges, and future prospects," in The Art of Digital Governance, Springer, 2025, doi: 10.1007/978-3-032-00514-4_13.
19. M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," BMJ, vol. 372, p. n71, 2021, doi: 10.1136/bmj.n71.
20. Q. N. Hong et al., "The Mixed Methods Appraisal Tool (MMAT) version 2018," Education for Information, vol. 34, no. 4, pp. 285–291, 2018, doi: 10.3233/EFI-180221.
21. B. J. Shea et al., "AMSTAR 2: A critical appraisal tool for systematic reviews," BMJ, vol. 358, p. j4008, 2017, doi: 10.1136/bmj.j4008.
22. J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," Biometrics, vol. 33, no. 1, pp. 159–174, 1977.
23. C. Aldemir and T. U. Uysal, "Artificial intelligence for financial accountability and governance in the public sector," Admin. Sci., vol. 15, no. 2, p. 58, 2025, doi: 10.3390/admsci15020058.
24. ENISA, "ENISA Artificial Intelligence Threat Landscape," European Union Agency for Cybersecurity, 2023. [Online]. Available: https://www.enisa.europa.eu
25. European Parliament, "Regulation (EU) 2016/679 (General Data Protection Regulation)," OJ L 119, Apr. 2016.
26. P. Kairouz et al., "Advances and open problems in federated learning," Foundations and Trends in ML, vol. 14, no. 1–2, pp. 1–210, 2021, doi: 10.1561/2200000083.
27. M. D. Wilkinson et al., "The FAIR Guiding Principles for scientific data management," Scientific Data, vol. 3, p. 160018, 2016, doi: 10.1038/sdata.2016.18.
28. D. Kreuzberger, N. Kühl, and S. Hirschl, "Machine learning operations (MLOps): Overview, definition, and architecture," IEEE Access, vol. 11, pp. 31866–31879, 2023, doi: 10.1109/ACCESS.2023.3262138.
29. A. B. Arrieta et al., "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges," Information Fusion, vol. 58, pp. 82–115, 2020, doi: 10.1016/j.inffus.2019.12.012.

 doi:10.20944/preprints202606.0428.v1

30. M. Mitchell et al., "Model cards for model reporting," in Proc. ACM FAccT, 2019, pp. 220–229, doi: 10.1145/3287560.3287596.
31. T. Gebru et al., "Datasheets for datasets," Commun. ACM, vol. 64, no. 12, pp. 86–92, 2021, doi: 10.1145/3458723.
32. CISA, "JCDC AI Cybersecurity Collaboration Playbook," CISA, 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/jcdc-ai-cybersecurity-collaboration-playbook
33. Verizon, "Data Breach Investigations Report 2024," Verizon Business, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir
34. European Parliament and Council, "Directive (EU) 2022/2555 on Cybersecurity (NIS2 Directive)," OJ L 333, Dec. 2022.
35. Office of Management and Budget, "M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of AI," OMB, Washington, DC, 2024.
36. NIST, "Computer Security Incident Handling Guide," SP 800-61r3, 2024, doi: 10.6028/NIST.SP.800-61r3.
37. D. Sculley et al., "Hidden technical debt in machine learning systems," in Proc. Advances in Neural Information Processing Systems (NIPS), 2015, pp. 2503–2511.
38. Open Cybersecurity Schema Framework (OCSF), "OCSF Schema Specification v1.0," 2023. [Online]. Available: https://schema.ocsf.io