ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Information Governance as a Dynamic Capability for Data-Driven AI Innovation: A Systematic Literature Review

Ahmad Faza | Information System, Universitas Multimedia Nusantara, Indonesia | ORCID: 0000-0003-0767-1053

Ilyana Agri Lestari | Department of Social Welfare, University of Indonesia, Indonesia | ORCID: 0000-0002-2753-0170

Abstract

Artificial intelligence (AI)-enabled systems, such as large language models (LLMs) and federated learning, are fundamentally transforming organisational workflows into distributed, model-centric ecosystems. While these advancements drive innovation, they simultaneously heighten information governance (IG) challenges regarding data privacy, algorithmic accountability, and systemic transparency. Although various ethical frameworks have been proposed to address these concerns, their practical operationalisation remains fragmented across different sectors. This study addresses this gap through a PRISMA 2020 guided systematic review of 78 peer-reviewed studies published between 2020 and 2024, aiming to synthesise a cohesive architecture for modern AI governance. The review identifies five core IG functions essential for maintaining integrity: accountability, data quality, privacy-by-design, compliance, and risk management. These functions are not merely theoretical; they are enabled by six distinct technological clusters, including privacy-preserving federated learning, machine-learning operations (MLOps), and AI–blockchain traceability. These tools allow organisations to move beyond manual oversight towards automated, scalable governance. Furthermore,

Received: 9.03.2026

Accepted: 30.06.2026

Published: 24.08.2026

Cite this article as:
A. Faza, I.A. Lestari "Information governance as a dynamic capability for data-driven AI innovation: A systematic literature review," ACIG, vol. 5, no. 2, 2026, doi: 10.60097/ACIG/225267.

Corresponding author:
Ahmad Faza, Information System, Universitas Multimedia Nusantara, Indonesia; Email: ahmad.faza@umn.ac.id
0000-0003-0767-1053

the research highlights that human governance must be distributed across ethical oversight and technical validation. This necessitates a multidimensional competency architecture that spans legal awareness, analytical proficiency, and socio-technical skills. Ultimately, IG is evolving from a reactive, *post hoc* compliance exercise into a proactive, lifecycle-oriented socio-technical capability. By integrating advanced technological clusters with human-centred agency, organisations can bridge the gap between abstract ethical principles and the practical, distributed demands of modern AI governance. This holistic shift ensures the creation of robust, transparent, and secure information ecosystems that are resilient to the complexities of the digital age.

Keywords

information governance, AI-enabled systems, socio-technical capability, privacy-by-design

1. Introduction

Artificial intelligence (AI)-enabled systems, such as automation, data-driven decision-making, large language models (LLMs), and cyber-physical architectures, are reshaping organisational processes through distributed and model-centric information flows. This review focuses on data-driven and model-centric AI-enabled systems because this is where the reviewed information governance (IG) literature is most concentrated. These systems reconfigure how organisations coordinate work, manage inter-organisational data exchange, and embed algorithmic outputs into operational decisions [1, 2]. Algorithmic intelligence now augments human judgement in sectors, such as healthcare, manufacturing, public administration, and digital services, improving responsiveness while also increasing governance complexity [3, 4].

At the same time, the scale, velocity, and heterogeneity of data in AI-driven environments have altered how information is generated, interpreted, reused, and controlled. Modern AI relies on high-velocity data streams across clinical, regulatory, and cyber-physical domains [5, 6]. Privacy risks are increasingly embedded in inferred knowledge produced by models, even when explicit identifiers are removed [7]. Although federated learning and related privacy-enhancing technologies can reduce direct data exposure, distributed pipelines introduce new privacy-utility trade-offs, accountability challenges, and coordination demands [8, 9]. Automated curation and metadata governance have therefore become essential for maintaining data quality, Findability, Accessibility, Interoperability, and Reusability (FAIR) alignment, and lifecycle-level traceability [10].

These developments introduce IG challenges that go beyond traditional data management. The opacity of AI architectures creates new vectors for privacy leakage, while accountability becomes diffused across algorithms, developers, organisational decision makers, domain experts, and end users [11, 12]. Data quality deficiencies further undermine explainability, necessitating automated quality control and standardisation [13]. In high-risk domains, reliance on black-box models constrains deployment, motivating the need for explainable AI (XAI) and the management of interpretive trade-offs [14].

Consequently, IG has evolved from a technical control function into a socio-technical organisational challenge. Effective governance requires the continuous integration of technical safeguards with human judgement, organisational capability, and ethical deliberation [15, 16]. Accountability is socially constructed through governance tools, role allocations, and institutional procedures rather than being solely embedded in system design [17]. In practice, socio-technical IG is instantiated through workflow-level design choices and interdisciplinary arrangements that combine AI tools with expert judgement [18, 19].

This study frames AI-enabled IG through dynamic capability theory. Dynamic capabilities refer to an organisation's capacity to sense environmental change, seize opportunities and risks through strategic action, and reconfigure resources, routines, and competencies as conditions evolve [20–22]. This framing is appropriate because AI governance challenges are not static. They require organisations to detect emerging data, model, regulatory, and accountability risks, embed governance controls into AI workflows, and revise roles and competencies as technologies and institutional expectations change.

Prior scholarship defines AI governance (AIG) as a multidimensional system aligning AI deployment with organisational strategy and ethics [23]. The existing reviews have advanced the field by mapping AI governance themes, ethical frameworks, and data governance mechanisms [24–26]. However, they provide limited explanation of how IG functions, AI technologies, human roles, and professional competencies operate together as a dynamic organisational capability. This review addresses that gap by synthesising the operational mechanisms through which governance is enacted across the AI lifecycle and by linking them to sensing, seizing, and reconfiguring processes.

- Research question (RQ)1: What IG functions are implemented in AI-enabled systems across different sectors?
- RQ2: What AI technologies and methods are utilised to support IG processes?
- RQ3: What are the human roles and responsibilities in managing IG within AI-enabled systems?
- RQ4: What skill sets and competencies are required for professionals to effectively govern these systems?

In this review, IG is conceptualised as an organisational capability encompassing structures, processes, roles, and competencies that regulate information across the AI system lifecycle within AI-enabled socio-technical systems. AI-enabled socio-technical systems are defined as AI applications embedded in organisational, regulatory, and human workflows where technical components interact with institutional roles, policies, and social practices. The term 'AI-enabled systems' in this paper refers primarily to data-driven and model-centric systems, while symbolic, knowledge-based, and hybrid neuro-symbolic AI are discussed as an important boundary condition and future research direction.

The study therefore makes three contributions. First, it consolidates IG functions across sectors rather than treating governance as a purely technical or legal issue. Second, it integrates technological enablers with human roles and competencies to address the implementation gap in AI governance. Third, it develops a theory-oriented interpretation of AI-enabled IG as a dynamic capability that connects governance mechanisms with organisational sensing, seizing, and reconfiguring.

2. Literature Review

2.1. The Changing Landscape of Information Governance in AI-Enabled Systems

The rapid diffusion of data-driven AI-enabled systems has reshaped the scope of IG. As organisations increasingly operate through distributed, model-centric, and data-intensive architectures, governance challenges extend beyond conventional data management towards accountability, privacy, transparency, reliability, and lifecycle traceability. This shift is visible in healthcare, Industry 4.0, urban mobility, and cyber-physical environments, where heterogeneous and high-velocity data intensify governance complexity and magnify the risks of automated decision-making [5, 27–29]. Privacy threats are no longer confined to explicit identifiers, because AI systems can infer sensitive attributes from anonymised data, thereby challenging lawful use, integrity, and control of information [1, 30, 31]. Cloud-based LLMs and multi-agent generative AI further intensify these concerns by introducing opaque decision pathways and cross-organisational data flows [18]. Within this landscape, IG in AI-enabled systems is operationalised through interdependent functions designed to sustain trustworthy and compliant operation, including privacy protection, accountability and transparency, data quality assurance, regulatory compliance, and risk management. These functions are supported by technologies such as homomorphic encryption, differential privacy, federated learning, blockchain-based provenance, and XAI [14, 27, 32, 33]. AI has also become an enabler of governance by automating information extraction, document classification, audit preparation, and sensitive-content detection through natural language processing (NLP), machine learning (ML), and LLM-based workflows [34–37]. Accordingly, governance is no longer only imposed on AI infrastructures from outside, it is increasingly embedded within the infrastructures, pipelines, and workflows through which AI systems operate.

2.2. Human-Centred Governance and the Implementation Gap

Despite the growth of technical governance mechanisms, the reviewed literature repeatedly shows that AI-enabled IG cannot be reduced to privacy technologies, audit tools, or compliance checklists. Governance is enacted through people who define acceptable risk, interpret model outputs, allocate accountability, translate legal requirements into workflows, and decide when automated systems should be trusted, challenged, or constrained. This human-centred dimension is especially visible in high-stakes contexts, such as clinical decision support, public administration, and legal or auditing environments, where domain experts, managers, regulators, auditors, and affected communities mediate between technical system behaviour and institutional responsibility [16, 38–42]. The implementation gap therefore concerns not only the absence of governance tools but also the absence of clear role architectures, escalation pathways, cross-functional competencies, and feedback loops through which governance can adapt as AI systems evolve. Prior work identifies developer-centric bias as a persistent weakness because responsible AI tools often emphasise technical builders while underrepresenting organisational leaders, domain specialists, users, and communities affected by AI decisions [42].

A human-centred IG perspective responds to this gap by treating governance as a socio-technical practice distributed across technical, managerial, legal, ethical, and operational actors. This provides the basis for examining IG as a capability that must be learned, maintained, and reconfigured rather than as a fixed compliance routine.

2.3. Dynamic Capability Theory and Information Governance

Dynamic capability theory distinguishes adaptive organisational capabilities from ordinary operational routines. Teece et al. conceptualise dynamic capabilities as the capacity to integrate, build, and reconfigure internal and external competences in response to rapidly changing environments [20]. Eisenhardt and Martin further argue that dynamic capabilities consist of identifiable processes, such as product development, strategic decision-making, and alliancing, whose value depends on how they help organisations adapt under changing conditions [21]. Teece later specifies the microfoundations of dynamic capabilities as sensing, seizing, and reconfiguring [22].

This distinction is important for the present review because not every governance routine is dynamic. Codified policies, audit forms, and compliance workflows may stabilise organisational behaviour, but they become dynamic capabilities only when they enable organisations to detect changing AI-related risks, convert those signals into governance action, and reconfigure technical, procedural, and human resources. In AI-enabled IG, sensing includes detecting data quality failures, privacy leakage, model drift, accountability gaps, and regulatory change. Seizing includes embedding privacy-preserving architectures, explainability tools, audit mechanisms, and role allocations into AI workflows. Reconfiguring includes revising governance structures, professional competencies, and workflow responsibilities as technologies and institutional expectations evolve. This framework anchors the review's claim that IG can function as a dynamic capability rather than merely as a static compliance instrument.

2.4. Previous Works

Prior studies on AIG define governance as a multidimensional system aligned with organisational strategy and ethical principles [23, 24]. Related reviews have mapped AI governance principles, responsible AI tools, ethical frameworks, and general data governance mechanisms [24–26, 42]. However, these reviews tend to emphasise either broad governance themes, ethical principles, or data governance concepts while offering limited synthesis of how operational IG functions, AI technologies, human roles, and competencies interact as a dynamic organisational capability. The present study therefore focuses on implementation-oriented IG within data-driven AI-enabled systems and positions human agency, technical enablers, and organisational adaptation as interdependent elements of governance. As shown in Figure 1 and Tables 1 and 2, prior research is concentrated in theoretical,

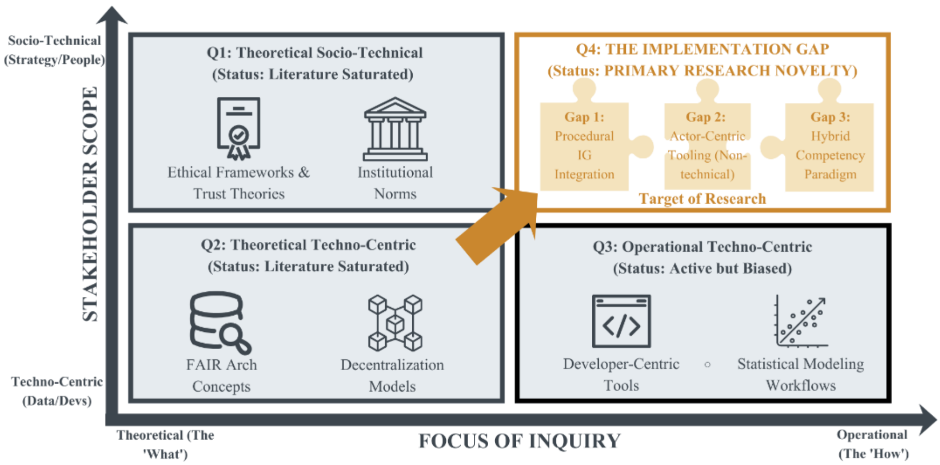

Figure 1. Strategic mapping of research maturity and target novelty area.

Table 1. Positioning of the present review against related reviews.

Related review	Primary focus	Remaining gap for this study	Present study's contribution
Birkstedt et al. [23]	AI governance themes, knowledge gaps, and future agendas.	Provides broad AI governance mapping but less operational detail on information governance (IG) functions, roles, and competencies.	Links IG functions, technologies, roles, and competencies to operational governance capability.
Batool et al. [24]	Systematic review of AI governance concepts and dimensions.	Covers overlapping governance territory but does not theorise IG as a dynamic capability.	Develops a dynamic capability interpretation using sensing, seizing, and reconfiguring.
Kuehnert et al. [42]	Responsible AI governance tools by actor and AI lifecycle stage.	Identifies actor–stage bias but is less focused on IG as an organisational capability across sectors.	Extends actor analysis towards cross-functional human roles and competency clusters.
Ismail and Ahmad [25]	Ethical and governance frameworks for AI.	Strong on governance principles but weaker on implementation mechanisms and human role architectures.	Synthesises implementation mechanisms and socio-technical governance responsibilities.
Bližnák et al. [26]	Recent data governance literature.	Focuses on data governance broadly rather than AI-enabled IG and model-centric governance.	Specifies how data governance concerns become lifecycle IG issues in AI-enabled systems.

Table 2. Synthesis matrix of contemporary AI-enabled information governance (IG) studies across sectors.

Focus and IG functions	Technologies and methods	Human agency and skills	Critical gap/synthesis	Sources
Lifecycle Audit and policy: risk mitigation and strategic alignment	TOE framework; risk-tiered regulatory and policy tools	Multi-tier accountability (team to national)	Decision gap: lack of guidance for tool selection	[25, 42]
Clinical AI: FAIR principles, data quality, and clinical safety	Hybrid data lakehouses; clinical decision support system (CDSS); Digital tumour boards	Clinicians and leaders; human-centric care skills	Implementation gap: lack of operational procedures	[38, 43, 44]
Responsible AI: decentralised privacy and accountability	Blockchain; federated learning; smart contracts	Critiques developer bias; excludes non-tech leaders	Actor imbalance: tools neglect leaders and end-users	[42, 45]
Digital audit: public sector accountability and monitoring	AI-driven real-time monitoring and reporting	Auditors and administrative leaders; tech agility	Regulatory gap: lacks international coordination	[39, 46]
Public trust: citizen engagement and service interaction	Explainable AI (XAI); trust transfer mechanisms	Citizens and political leaders; digital literacy	Socio-technical gap: trust requires human 'bridges'	[47–49]
Business IG: Data asset valuation and asset compliance	System decomposition; business artificial intelligence governance (AIG) frameworks	Novel governance roles; board of directors	Practicality gap: operational ambiguity in business	[26, 50]
Predictive justice: efficiency and oversight in legal sectors	Justice 5.0; collaborative decision-making tools	Legal professionals vs. 'Robot Judges' concepts	Ethical risk: rrosion of judicial discretion	[51]
IT Maturity: strategic resource and IT risk control	BDG MAM (maturity model); 5V big data management	Board-level committees; proactive AI mindset	Hybrid paradigm: shift from 'knowing' to application	[52, 53]

ethical, or techno-centric domains, while implementation-oriented work remains fragmented across sectors and often focused on developer-centric tools. Consequently, a major gap persists in integrating procedural IG implementation, non-technical actors, and hybrid competencies within a unified socio-technical governance perspective across the AI lifecycle.

3. Method

This review followed Kitchenham's three-phase framework of planning, conducting, and reporting to ensure rigour and reproducibility, while Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) 2020 guided transparent identification, screening, eligibility assessment, and reporting procedures [54–57]. The two frameworks were used for complementary purposes rather than as competing methodologies: Kitchenham structured the systematic review protocol and quality appraisal process, whereas PRISMA 2020 documented how records moved through identification, screening, eligibility, and inclusion. During planning, a review protocol specified the research questions, search strategy, inclusion and exclusion criteria, and quality assessment criteria (Figure 2). Study quality was appraised using established systematic literature review (SLR) guidelines, focusing on theoretical grounding, methodological rigour, clarity of objectives, credibility of findings, and contribution to the knowledge base [56, 58–60].

A pilot test of 10 studies refined keywords before the search. The search was conducted in January 2025 and covered publications from 2020 to January 2025, including early-online 2025 studies available at the time of retrieval. Databases included IEEE Xplore, ACM Digital Library, AAAI Digital Library, ScienceDirect, SpringerLink, Wiley Online Library, Taylor & Francis Online, SAGE Journals, and Emerald Insight, with supplementary snowballing used to reduce omission bias [61–65]. Scopus was not used as a primary search database because the protocol prioritised full-text and publisher-level retrieval from AI, computing, governance, and multidisciplinary databases. This decision may have limited coverage of organisational behaviour and management journals indexed primarily in Scopus, and it is acknowledged as a limitation.

A total of 4250 records were retrieved, of which 1350 were removed before screening because of duplication and metadata issues, leaving 2900 records for title and abstract screening. After excluding 2617 records and assessing 258 reports for eligibility, 78 studies met all inclusion criteria and were retained for final synthesis (Figure 3). To strengthen screening objectivity, two reviewers independently screened a random verification subset of 113 records. Inter-rater reliability yielded Cohen's kappa = 0.82, indicating overall strong agreement [66]. Discrepancies were resolved through discussion until consensus was reached. Table 3 reports the agreement statistics. Data were analysed through thematic synthesis informed by Braun and Clarke's thematic analysis [67–69]. In this review, thematic analysis was applied to extracted secondary evidence, not to primary interview or observation data. Coding focused on IG functions, enabling AI technologies and methods, human roles and responsibilities, and competencies required for effective

<table>
<tr><th>Section</th><th>Source Text</th></tr>
<tr><td>Research Questions</td><td>• What information governance (IG) functions are implemented in AI-enabled systems across different sectors?
• What AI technologies and methods are utilized to support information governance processes?
• What are the human roles and responsibilities in managing IG within AI-enabled systems?
• What skillsets and competencies are required for human professionals to effectively govern and manage AI-enabled information systems?</td></tr>
<tr><td>Search Strategy</td><td>
<table>
<tr><th></th><th>Digital Library</th><th>URL</th></tr>
<tr><td rowspan="14">Digital Libraries</td><td>ScienceDirect</td><td>https://www.sciencedirect.com/</td></tr>
<tr><td>Scopus</td><td>https://www.scopus.com/</td></tr>
<tr><td>IEEE Xplore</td><td>https://ieeexplore.ieee.org/</td></tr>
<tr><td>SpringerLink</td><td>https://link.springer.com/</td></tr>
<tr><td>MDPI</td><td>https://www.mdpi.com/</td></tr>
<tr><td>Wiley Online Library</td><td>https://onlinelibrary.wiley.com/</td></tr>
<tr><td>AAAI Digital Library</td><td>https://aitdl.aaai.org/</td></tr>
<tr><td>ACM Digital Library</td><td>https://dl.acm.org/</td></tr>
<tr><td>Nature Portfolio</td><td>https://www.nature.com/</td></tr>
<tr><td>Frontiers</td><td>https://www.frontiersin.org/</td></tr>
<tr><td>SAGE Journals</td><td>https://journals.sagepub.com/</td></tr>
<tr><td>Emerald Insight</td><td>https://www.emerald.com/</td></tr>
<tr><td>Taylor & Francis Online</td><td>https://www.tandfonline.com/</td></tr>
<tr><td rowspan="5">Search terms</td><td>Keywords</td><td>Alternatives</td></tr>
<tr><td>information governance</td><td>data governance</td></tr>
<tr><td>artificial intelligence</td><td>AI-enabled systems</td></tr>
<tr><td>functions</td><td>processes</td></tr>
<tr><td>human roles</td><td>competencies</td></tr>
<tr><td>Search String</td><td colspan="2">(“information governance” OR “data governance”)
AND (“artificial intelligence” OR “AI-enabled systems”)
AND (functions OR processes)
AND (“human roles” OR competencies)</td></tr>
</table>
</td></tr>
<tr><td>Inclusion Criteria</td><td>• Peer-reviewed full-text journal articles
• Published between 2020 and 2025
• Written in English
• Accessible via open access or institutional access
• Explicitly address information governance or data governance in organizational or socio-technical contexts
• Examine AI-enabled systems or the use of artificial intelligence in governance-related processes
• Identify governance functions or processes supported, automated, or transformed by AI
• Discuss human involvement, including roles, responsibilities, skills, or competencies in governing or managing AI-enabled information systems</td></tr>
<tr><td>Exclusion Criteria</td><td>• Grey literature, including theses, dissertations, unpublished, or incomplete works
• Books, book chapters, editorials, opinion pieces, and non-peer-reviewed publications
• Studies not focused on information or data governance, even if AI is discussed
• AI studies without governance-related functions or processes
• Studies excluding human roles, responsibilities, or competencies in AI governance
• Purely technical AI studies (e.g., algorithm design, model optimization, benchmarking) without organizational, ethical, or governance context</td></tr>
<tr><td>Quality Criteria</td><td>• Theoretical basis: Clear grounding in relevant theories, frameworks, or conceptual models related to information governance, AI, or socio-technical systems.
• Research objectives: Clearly stated and well-defined research aims aligned with the study design and scope.
• Data gathering, analysis, and presentation: Transparent and appropriate methods for data collection, analysis, and reporting, with sufficient detail to support reproducibility or methodological rigor.
• Reference use: Use of relevant, up-to-date, and credible scholarly references that support theoretical and methodological claims.
• Credibility of findings and stated conclusions: Logical consistency between data, analysis, and conclusions, with limitations acknowledged where appropriate.
• Contribution to knowledge or understanding: Explicit contribution to theory, practice, or understanding of information governance, AI-enabled systems, or human governance roles.</td></tr>
</table>

Figure 2. Systematic literature review (SLR) protocol and study selection criteria.

Table 3. Inter-rater reliability summary for manuscript screening.

Metric	Value	Explanation
Double-screened verification subset	113 records	Random subset used to assess screening consistency.
Agreements	106	Records for which both reviewers reached the same include/exclude decision.
Disagreements	7	Records requiring discussion and consensus resolution.
Percentage agreement	93.8%	Calculated as 106/113.
Cohen's kappa	0.82	Indicates strong inter-rater agreement according to Landis and Koch [66].
Resolution process	Consensus discussion	All disagreements were discussed until a final decision was agreed.

Table 4. Mapping of research questions (RQs) to thematic codes and evidence sources.

RQs	Codification	Source
What information governance (IG) functions are implemented in AI-enabled systems across different sectors?	Establishes model governance and validation mechanisms to ensure trustworthy and reliable AI systems.	P1: organisations are more likely to detect emergent AI governance risks when data quality, provenance, explainability, and risk monitoring are integrated into continuous review processes.
What IG functions are implemented in AI-enabled systems across different sectors?	Promotes transparency and explainability to enhance accountability and user trust.	P1
What IG functions are implemented in AI-enabled systems across different sectors?	Defines human-in-the-loop role delineation to maintain oversight in automated processes.	P1
What IG functions are implemented in AI-enabled systems across different sectors?	Emphasises high data quality and consistent labelling standards for robust AI performance.	P1
What IG functions are implemented in AI-enabled systems across different sectors?	Implements bias and risk assessment as part of ethical AI evaluation.	P1

governance. The analysis followed the following six stages: familiarisation with included studies, initial coding, theme development, theme review, theme definition, and final synthesis. Table 4 links research questions with coded interpretations, original evidence, and source studies, while Table 5 illustrates how lower-level codes were aggregated into higher-level categories and overarching themes.

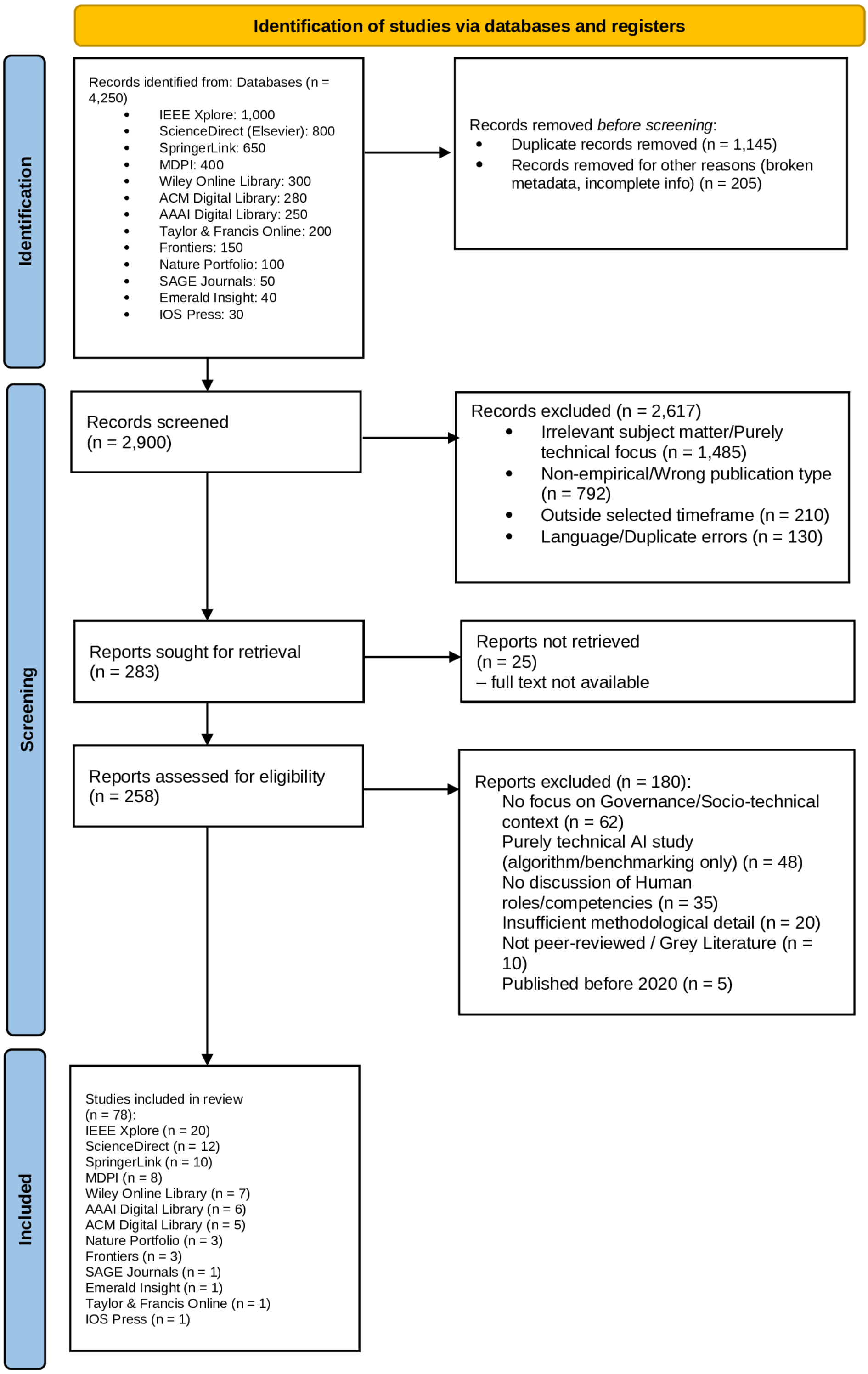

Figure 3. The Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) flow diagram of the study selection process.

Table 5. Illustrative example of the qualitative codification process mapping specific competencies to thematic domains.

Competency / Skill	Mapped Category	Overarching Proficiency Domain
Maintains regulatory literacy on GDPR/HIPAA	Regulatory Compliance & Privacy	Ethical & Governance Literacy
Applies data annotation for privacy	Regulatory Compliance & Privacy	Ethical & Governance Literacy
FOIA & privacy ethics	Regulatory Compliance & Privacy	Ethical & Governance Literacy
Understands PDPA regulations	Regulatory Compliance & Privacy	Ethical & Governance Literacy
Bias and fairness awareness	AI Ethics & Fairness	Ethical & Governance Literacy
Ethics policy literacy	AI Ethics & Fairness	Ethical & Governance Literacy
Risk-based incident handling	AI Ethics & Fairness	Ethical & Governance Literacy
Balances algorithmic accuracy with ethics	AI Ethics & Fairness	Ethical & Governance Literacy
Data governance standards (COSO/IIA)	Governance Frameworks	Ethical & Governance Literacy
Audit readiness skills	Governance Frameworks	Ethical & Governance Literacy
Responsible AI workflows	Governance Frameworks	Ethical & Governance Literacy
Accountability skills	Governance Frameworks	Ethical & Governance Literacy
IP and FDA law literacy	Legal & IP Literacy	Ethical & Governance Literacy
Translating complex legal text to rules	Legal & IP Literacy	Ethical & Governance Literacy
Medical consent laws	Legal & IP Literacy	Ethical & Governance Literacy
R programming workflows	Advanced ML & Data Engineering	Technical & Analytical Proficiency
NLP (Word2Vec) techniques	Advanced ML & Data Engineering	Technical & Analytical Proficiency
ML ensemble algorithms	Advanced ML & Data Engineering	Technical & Analytical Proficiency
Data preprocessing and feature engineering	Advanced ML & Data Engineering	Technical & Analytical Proficiency
Differential privacy engineering	Security & Privacy Tech	Technical & Analytical Proficiency
Cryptography literacy	Security & Privacy Tech	Technical & Analytical Proficiency
AI-driven threat analysis	Security & Privacy Tech	Technical & Analytical Proficiency
Secure protocol design	Security & Privacy Tech	Technical & Analytical Proficiency
Model interpretability competence	Explainable AI (XAI)	Technical & Analytical Proficiency
XAI development	Explainable AI (XAI)	Technical & Analytical Proficiency
UI trust monitoring	Explainable AI (XAI)	Technical & Analytical Proficiency
AI performance metrics evaluation	Explainable AI (XAI)	Technical & Analytical Proficiency
Cloud infrastructure management	System Architecture & QA	Technical & Analytical Proficiency
ISO/IEC 25010 QA standards	System Architecture & QA	Technical & Analytical Proficiency
Site Reliability Engineering (SRE)	System Architecture & QA	Technical & Analytical Proficiency
Industrial process integration	System Architecture & QA	Technical & Analytical Proficiency

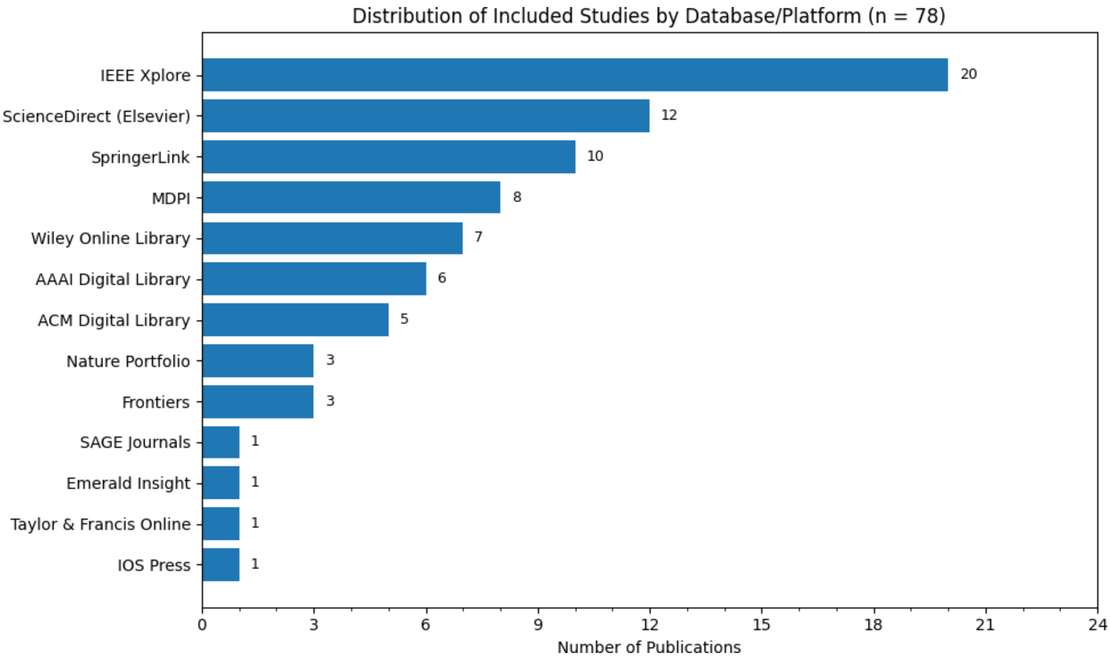

Figure 4. Distribution of included studies across digital libraries and publishers.

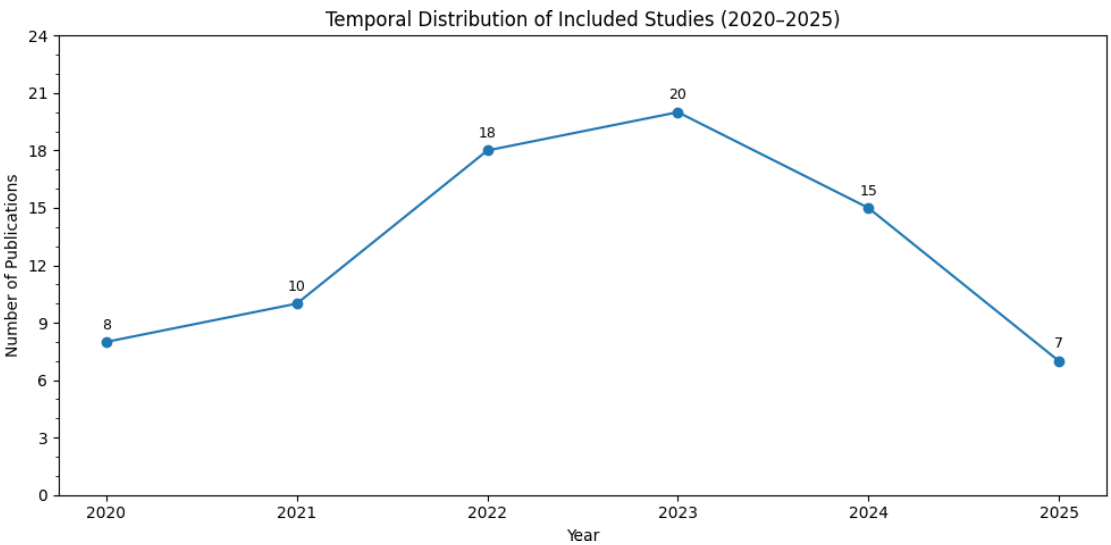

Figure 5. Publication trend of AI-enabled information governance (IG) research over the study period.

4. Results

This review synthesised 78 peer-reviewed studies published between 2020 and January 2025 to map the operational landscape of AI-enabled information governance. The corpus shows a marked increase in publications after 2021, indicating growing institutional attention to governance challenges in distributed and model-centric AI environments (Figs. 5 and 6). Compared with an earlier work centred on abstract ethical principles, the reviewed studies reflect a shift towards operational governance mechanisms embedded in real organisational settings. The findings are organised into four interrelated domains: governance functions, enabling technologies, human roles and responsibilities, and professional competencies. Only representative references are shown in the main text tables, while the full study-to-theme mapping is provided in the Supplementary Material.

4.1. Mapping IG Functions

Studies identify five recurring IG functions across the AI data and model lifecycle: accountability and transparency, data quality and integrity, ethical and privacy-by-design governance, compliance and audit assurance, and security and risk management. Across the reviewed sectors, the most consistently emphasised functions are accountability, data quality, and privacy-oriented governance, reflecting shared concerns with traceability, reliability, and lawful data use in increasingly distributed AI environments. Accountability and transparency are typically operationalised through model explanation tools, provenance capture, and process documentation that support reviewability and *post hoc* justification [70–72]. In parallel, data quality and integrity are treated as foundational to institutional trust, with studies highlighting metadata governance, audit trails, and alignment with FAIR and International Organization for Standardization (ISO) standards to preserve accuracy across the lifecycle [10, 73, 74]. Ethical and privacy-by-design mechanisms further reinforce these functions by embedding fairness, consent, and explainability into both design-time and run-time governance through approaches such as federated learning, differential privacy, and institutional review board (IRB)-aligned oversight [13, 31, 75].

The remaining functions, namely compliance and audit assurance, and security and risk management, most often appear as mechanisms that institutionalise and sustain these core governance priorities under sector-specific constraints. In healthcare, IG functions are closely tied to patient safety, privacy protection, and visible

Table 6. Thematic summary of information governance (IG) functions.

Theme	No. of studies	Representative references
Accountability and transparency	55	[14, 17, 70]
Data quality and integrity	55	[10, 73, 74]
Ethical governance and privacy	34	[1, 31, 75]
Compliance and audit assurance	9	[19, 82, 83]
Security and risk management	5	[12, 30, 33]

human oversight; in industrial settings, they are oriented towards operational resilience, real-time monitoring, and document or process traceability; while in public administration, they are linked more strongly to auditability, regulatory legitimacy, and formal accountability structures [19, 29, 76, 77]. Across these contexts, compliance is commonly enacted through data protection impact assessments (DPIAs), telemetry, and human-in-the-loop controls aligned with General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or the European Union (EU) AI Act, whereas security and risk management support prevention, detection, and response through access governance, anomaly detection, privacy budgets, and tamper-evident controls [17, 78–80]. However, the literature also reveals unresolved tensions, particularly fragmented accountability structures, uneven governance maturity, and persistent trade-offs between transparency, confidentiality, and operational efficiency in distributed deployments [9, 15, 35, 81]. Table 6 summarises the thematic mapping of these IG functions, while the complete study-to-theme mapping is provided in Table S1.

4.2. Mapping AI Technologies Supporting Information Governance

Studies identify six recurring technological clusters that support IG in AI-enabled systems: privacy-preserving collaboration through federated learning, ethical and responsible AI design in machine-learning operations (MLOps), AI–blockchain integration, ML for anomaly detection, deep learning for information extraction, and AI-driven risk assessment. Across the literature, the dominant patterns are privacy-preserving collaboration, governance-by-design in MLOps, and infrastructure-level traceability, indicating that AI-enabled IG is increasingly operationalised through distributed, auditable, and privacy-aware architectures. Federated learning and related privacy-enhancing technologies are the most frequently reported enablers, supporting model training without raw data exchange through differential privacy, homomorphic encryption,

Table 7. Thematic summary of AI technologies supporting information governance.

Theme	No. of studies	Representative references
Federated learning and data heterogeneity	48	[31, 81, 84]
Ethical and responsible AI design	37	[14, 83, 88]
AI–Blockchain integration for traceability and IP protection	20	[1, 29, 86]
Machine learning (ML) for anomaly and fraud detection	15	[9, 90, 92]
Deep learning for information extraction and leak detection	7	[35, 70, 93]
AI for risk assessment and security	6	[16, 17, 79]

secure multiparty computation, and adaptations for heterogeneous environments [31, 81, 84, 85]. Ethical and responsible AI design complements these mechanisms by embedding fairness-aware learning, explainability, accountability-by-design, and continuous monitoring within MLOps pipelines, while AI–blockchain integration strengthens provenance, consent automation, and decentralised trust across organisational boundaries [11, 12, 29, 83, 86–88].

The remaining clusters, namely anomaly detection, information extraction, and AI-driven risk assessment, mainly function as operational tools for monitoring, multimodal oversight, and adaptive security response. Their emphasis varies by context: anomaly detection is more prominent in transactional and infrastructure-heavy settings, information extraction in document-intensive and multimodal environments, and risk-assessment tools where policy verification and threat propagation require continuous tracking [9, 70, 79, 89, 90]. Across sectors, however, the literature highlights persistent tensions, including scalability and latency constraints in federated and blockchain-based systems, performance-interpretability trade-offs in fairness-aware and explainability-driven models, and the limited generalisability of monitoring tools across governance contexts [2, 28, 72, 91]. Taken together, these findings suggest that AI technologies increasingly embed governance logic within the technical infrastructure of AI systems rather than merely supporting it from the outside. Table 7 summarises the technological clusters supporting information governance, while the complete study-to-theme mapping is provided in Table S2.

4.3. Mapping Human Roles and Responsibilities in AI-Driven Governance Systems

The literature identifies five recurring role clusters in AI-enabled IG: ethical and governance oversight, technical development and validation, policy and regulatory frameworks, quality assurance and traceability, and system design and workflow integration. Across these clusters, the most dominant patterns are ethical oversight, technical validation, and regulatory coordination, showing that human involvement in AI governance is distributed across strategic, operational, and technical layers rather than concentrated in a single role. Ethical oversight remains central because developers, ethicists, and domain experts jointly sustain fairness, transparency, and professional accountability through human-in-the-loop arrangements, particularly in high-stakes contexts, such as healthcare and justice [31, 73, 94–96]. Technical development and validation roles support this oversight through reproducible architectures, fairness testing, drift detection, and privacy-preserving controls, while policy and regulatory roles translate ethical principles into enforceable mechanisms through legal obligations, consent requirements, and escalation pathways [17, 29, 36, 85, 97–99].

The remaining clusters, namely quality assurance and traceability, and system design and workflow integration, mainly function as operational mechanisms that embed governance into daily practice. Quality assurance roles emphasise audit trails, lineage records, and verification controls, whereas workflow integration roles embed governance requirements into development & operations (DevOps) and MLOps processes through interpretable interfaces and privacy-oriented system design [19, 30, 83, 86]. Their importance varies by context: regulated sectors prioritise traceability and formal accountability, while deployment-intensive settings emphasise integration and operational continuity. Across sectors, however, the literature highlights persistent tensions between rapid technical innovation and slower ethical or regulatory review as well as challenges in maintaining clear accountability across multiple actors and layers [1, 6, 8, 77]. Taken together, these findings

Table 8. Thematic summary of human roles and responsibilities in AI-driven governance systems.

Theme	No. of studies	Representative references
Ethical and governance oversight	71	[31, 94, 95]
Technical development and validation	64	[36, 85, 99]
Policy and regulatory frameworks	64	[17, 29, 97]
Quality assurance and traceability	25	[19, 71, 86]
System design and workflow integration	16	[83, 100, 101]

suggest that human roles in AI-enabled IG are best understood as an interconnected governance architecture rather than a set of isolated responsibilities. Table 8 summarises the human roles and responsibilities in AI-driven governance systems, while the complete study-to-theme mapping is provided in Table S3.

4.4. Mapping Competencies and Skill Sets within the AI-Enabled IG Domain

The reviewed studies identify five recurring competency clusters for governing AI-enabled information systems: ethical and governance literacy, collaborative and legal awareness, technical and analytical proficiency, experimental and evaluation skills, and human-centred socio-technical competence. Across these clusters, the most dominant capabilities are governance literacy, technical–analytical proficiency, and cross-functional legal collaboration, indicating that effective IG depends on the ability to connect ethical principles, regulatory requirements, and system performance in practice. Governance literacy is central because professionals must translate fairness, accountability, and privacy into operational controls, while technical–analytical proficiency supports system design, monitoring, validation, and the use of privacy-enhancing and explainability tools [10, 17, 89, 97, 99]. Collaborative and legal awareness further enables coordination across disciplines and jurisdictions, particularly in relation to GDPR, consent, and cross-border data governance [15, 18, 86, 102].

Experimental and evaluation skills, together with human-centred socio-technical competence, mainly appear as operational capabilities that sustain governance in practice. These include auditing privacy-utility trade-offs, testing robustness, calibrating trust, and aligning system design with organisational and cultural contexts [3, 11, 33, 70, 81, 103, 107]. Their relative emphasis varies by sector:

Table 9. Thematic mapping of competencies and skill sets within the AI-enabled information governance (IG) domain.

Theme	No. of studies	Representative references
Ethical and governance literacy	13	[17, 36, 97]
Collaborative and legal awareness	29	[15, 18, 86]
Technical and analytical proficiency	38	[72, 80, 104]
Experimental and evaluation skills	24	[14, 33, 81]
Human-centred and socio-technical competence	25	[3, 11, 103]

regulated environments prioritise legal literacy and auditability, whereas deployment-intensive settings stress technical validation and operational resilience. Across contexts, however, the literature reveals a persistent tension between rising governance complexity and the limited availability of professionals able to bridge compliance, engineering, and human-centred implementation. Taken together, these findings suggest that competency in AI-enabled IG is best understood as a hybrid capability architecture rather than a set of isolated skills. Table 9 summarises these competencies and skill sets, while the complete study-to-theme mapping is provided in Table S4.

5. Discussion

The findings of this SLR show that AI-enabled IG is evolving from a *post hoc* compliance activity into a distributed, lifecycle-spanning capability embedded within data-driven AI systems [15, 72]. This interpretation is not based merely on the observation that governance is important. Rather, it rests on how the four thematic domains identified in the review interact: governance functions define what must be controlled, technologies provide mechanisms for operationalising control, human roles allocate interpretive and accountability responsibilities, and competencies determine whether organisations can adapt those mechanisms under changing technical and institutional conditions.

Viewed through dynamic capability theory, the five IG functions identified in the review can be interpreted as a capability architecture. Data quality and integrity, accountability and transparency, and security and risk management contribute to sensing because they help organisations detect unreliable data, opaque models, privacy leakage, bias, drift, and emerging threats. Ethical governance, privacy-by-design, compliance, and audit assurance contribute to seizing because they translate detected risks into design choices, controls, and institutional commitments. Human-centred oversight, workflow integration, and competency development support reconfiguring because they enable organisations to revise governance routines, redistribute accountability, and update professional skills as AI systems and regulations evolve [20–22].

This mapping also addresses the critique that governance routines may be stable rather than dynamic. The review suggests that IG becomes dynamic only when stable routines, such as audit trails, DPIAs, data quality checks, and accountability documentation, are coupled with feedback mechanisms, monitoring tools, escalation

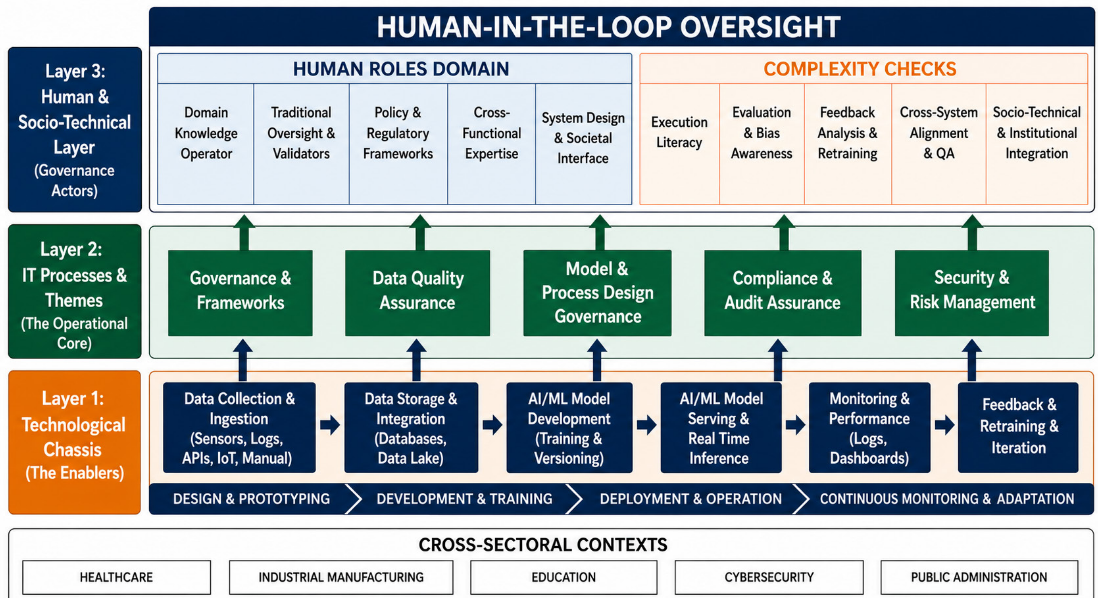

Figure 6. Thematic mapping of technological enablers, core functions, and human-centred governance roles within the AI-enabled information governance (IG) domain.

pathways, and cross-functional decision-making. Without these adaptive elements, governance remains an ordinary operational routine. With them, it becomes a capability for sensing changing conditions, seizing governance options, and reconfiguring socio-technical arrangements.

Figure 6 consolidates the thematic mapping of technological enablers, core IG functions, and human-centred governance roles within the AI-enabled IG domain. The figure should be read as an integrative map rather than a causal model: it shows where technical precision and human agency intersect, but the explanatory logic emerges from the capability interpretation developed below.

To move from taxonomy to theory-building, Table 10 translates the thematic synthesis into propositions that can guide future empirical research. These propositions specify how technologies may enable or constrain governance functions, how human roles mediate these relationships, and why organisational maturity conditions the effectiveness of IG as a dynamic capability.

These propositions extend the descriptive taxonomy by identifying configurational relationships among technologies, governance functions, roles, and competencies. They also preserve a boundary condition emphasised in the reviewed literature: if AI-enabled IG depends exclusively on advanced infrastructures such as blockchain or complex federated pipelines, organisations in resource-constrained environments may face technological path dependence. A co-evolutionary perspective is therefore needed, where technologies and professional capabilities mutually shape one another rather than assuming that technical adoption alone produces responsible governance.

Table 10. Dynamic capability synthesis and propositions for AI-enabled information governance (IG).

Dynamic capability mechanism	Related IG functions	Key technology and method clusters	Human roles and competencies	Theory-building proposition
Sensing	Data quality and integrity; accountability and transparency; security and risk management.	Anomaly detection, information extraction, explainable AI (XAI), risk assessment, metadata governance.	Auditors, domain experts, data stewards, security analysts, and governance leaders with analytical and ethical literacy.	P1: organisations are more likely to detect emergent AI governance risks when data quality, provenance, explainability, and risk monitoring are integrated into continuous review processes.
Seizing	Ethical governance and privacy; compliance and audit assurance.	Federated learning, differential privacy, homomorphic encryption, responsible MLOps, AI–blockchain traceability.	Legal, compliance, technical, and managerial actors able to convert governance signals into deployable controls.	P2: privacy-preserving and traceability technologies strengthen IG only when organisations can translate them into concrete design choices, accountability rules, and audit procedures.
Reconfiguring	Cross-functional accountability; workflow integration; competency development.	MLOps feedback loops, lifecycle documentation, workflow-level governance tools, adaptive monitoring.	Leaders, developers, domain experts, and users who can redistribute responsibilities and update governance routines.	P3: AI-enabled IG becomes a dynamic capability when organisations revise roles, workflows, and competencies in response to changes in data, models, regulation, and stakeholder expectations.
Boundary condition	Inclusive governance and organisational maturity.	Technology choices calibrated to sectoral risk, infrastructure maturity, and institutional capacity.	Stakeholders able to align governance tools with local constraints and affected communities.	P4: the effectiveness of AI-enabled IG depends on fit between technological complexity and organisational maturity; excessive dependence on advanced infrastructures may reproduce governance inequality.

6. Limitations and Future Research

This review has several limitations. First, although the manuscript uses the term AI-enabled systems, the included studies are dominated by data-driven, model-centric, and generative AI applications. Symbolic, knowledge-based, and hybrid neuro-symbolic AI also require IG, particularly in relation to rule bases, knowledge representation, explainability, ontology governance, and hybrid reasoning accountability. However, these streams were not systematically represented in the retrieved corpus. Future reviews should examine IG requirements in symbolic and hybrid AI explicitly, rather than assuming that governance mechanisms developed for data-driven AI fully transfer to these paradigms.

Second, Scopus was not included as a primary search database. The review mitigated this limitation through multiple publisher databases, multidisciplinary sources, and snowballing, but relevant organisational behaviour and management studies may still have been missed. Third, the thematic counts reported in the results should be interpreted as coded occurrences within the reviewed corpus, not as meta-analytic effect sizes. Finally, because this study is based on secondary literature, the propositions developed in the discussion require future empirical testing across sectors with different levels of technological and institutional maturity.

Finally, future research may connect AI-enabled IG with the broader IT governance capability and maturity-assessment tradition. Studies on governance capability in operational contract management, COBIT 2019 implementation in mineral mining, and COBIT 5 capability-level measurement show how governance capability can be operationalised through process assessment, control alignment, and organisational accountability in non-AI settings [104–106]. These studies should not be treated as direct evidence of AI-enabled IG, but they provide a useful bridge for developing sector-sensitive capability metrics that can later be adapted to AI governance contexts.

7. Conclusions

This SLR synthesises how IG is implemented within data-driven AI-enabled systems across technological, organisational, and human dimensions. By consolidating evidence from diverse sectors and stages of AI lifecycle, it provides a structured understanding of how governance functions are enacted in contemporary AI-driven environments.

The study conceptualises AI-enabled IG as a socio-technical dynamic capability by integrating fragmented literatures and identifying recurring patterns through which governance is operationalised. Rather than treating governance principles as abstract or institutionally detached constructs, the review demonstrates how accountability, transparency, privacy, trust, and compliance are mediated through the interplay of technological infrastructures, organisational arrangements, and human oversight roles.

The review also clarifies that IG becomes dynamic only when governance routines support sensing, seizing, and reconfiguring. This insight advances the literature by moving from taxonomic mapping towards propositions that can be tested in future empirical research. It positions AI-enabled IG as an organisational concern that extends beyond formal policies and regulatory compliance while also acknowledging the need for further work on symbolic, knowledge-based, and hybrid AI governance.

Acknowledgement

The authors would like to express their sincere appreciation to Universitas Multimedia Nusantara (UMN) for its institutional support and for providing an academic environment that facilitated the completion of this research. The authors also acknowledge the support of the university in promoting research and scholarly publication in the field of information systems and information governance.

References

[1] M. Letafati, S. Otoum, "Global differential privacy for distributed metaverse healthcare systems," in *2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)*, Piscataway, NJ: IEEE, 2023, pp. 1–8, doi: 10.1109/iMETA59369.2023.10294469.

[2] R.S. Peres, A. Manta-Costa, J. Barata, "Implementing privacy-preserving and collaborative industrial artificial intelligence," *IEEE Access*, vol. 11, pp. 74579–74589, 2023, doi: 10.1109/ACCESS.2023.3296143.

[3] N. Mohammadi, J. Bai, Q. Fan, Y. Song, Y. Yi, L. Liu, "Differential privacy meets federated learning under communication constraints," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22204–22219, 2021, doi: 10.1109/JIOT.2021.3101991.

[4] T. Gorji, H. M. Saeedi, E. Mushtaq, H. K. Zadeh, K. Husarik, S. M. Shahabi, J. Qin et al., "Federated learning for clients' data privacy assurance in food service industry," *Applied Sciences*, vol. 13, no. 16, Art. no. 9330, 2023, doi: 10.3390/app13169330.

[5] J. Mattioli, P.-O. Robic, E. Jesson, "Information quality: The cornerstone for AI-based industry 4.0," *Procedia Computer Science*, vol. 201, pp. 453–460, 2022, doi: 10.1016/j.procs.2022.03.059.

[6] C. Sánchez-Zas, V.A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J.I. Moreno, J. Berrocal, "Ontology-based approach to real-time risk management and cyber-situational awareness," *Future Generation Computer Systems*, vol. 141, pp. 462–472, 2023, doi: 10.1016/j.future.2022.12.006.

[7] L. Ni, P. Huang, Y. Wei, M. Shu, J. Zhang, "Federated learning model with adaptive differential privacy protection in medical IoT," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Art. no. 8967819, 2021, doi: 10.1155/2021/8967819.

[8] J. Greser, "Cybersecurity framework for synthetic data in training medical AI," *European Journal of Risk Regulation*, vol. 15, no. 4, pp. 903–911, 2024, doi: 10.1017/err.2024.74.

[9] A. Raza, K.P. Tran, L. Koehl, S. Li, "AnoFed: Adaptive anomaly detection for digital health using transformer-based federated learning and support vector data description," *Engineering Applications of Artificial Intelligence*, vol. 121, Art. no. 106051, 2023, doi: 10.1016/j.engappai.2023.106051.

[10] I. Mutlu, J. Hackermueller, J. Schor, "Automated curation of spatial metadata in environmental monitoring data," *Ecological Informatics*, vol. 86, Art. no. 103038, 2025, doi: 10.1016/j.ecoinf.2025.103038.

[11] J.J. Hatherley, "Limits of trust in medical AI," *Journal of Medical Ethics*, vol. 46, no. 7, pp. 478–481, 2020, doi: 10.1136/medethics-2019-105935.

[12] R. Shokri, M. Strobel, Y. Zick, "On the privacy risks of model explanations," in *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, New York, NY, USA: Association for Computing Machinery, 2021, pp. 231–241, doi: 10.1145/3461702.3462533.

[13] G. Elkhawaga, M. Abu-Elkheir, M. Reichert, "Explainability of predictive process monitoring results: Can you see my data issues?," *Applied Sciences*, vol. 12, no. 16, Art. no. 8192, 2022, doi: 10.3390/app12168192.

[14] C. Panigutti, A. Beretta, D. Fadda, F. Giannotti, D. Pedreschi, A. Perotti, S. Rinzivillo, "Co-design of human-centered, explainable AI for clinical decision support," *ACM Transactions on Interactive Intelligent Systems*, vol. 13, no. 4, pp. 1–35, 2023, doi: 10.1145/3587271.

[15] L. Floridi, J. Cowls, T.C. King, M. Taddeo, "How to design AI for social good: Seven essential factors," in *Ethics, Governance, and Policies in Artificial Intelligence,* L. Floridi, Ed. Cham: Springer, 2021, pp. 125–151, doi: 10.1007/s11948-020-00213-5.

[16] N. Rees, K. Holding, M. Sujan, "Information governance as a socio-technical process in the development of trustworthy healthcare AI," *Frontiers in Computer Science*, vol. 5, Art. no. 1134818, 2023, doi: 10.3389/fcomp.2023.1134818.

[17] J.-H. Schmidt, S.C. Bartsch, M. Adam, A. Benlian, "Elevating developers' accountability awareness in AI systems development," *Business & Information Systems Engineering*, vol. 67, no. 1, pp. 109–135, 2025, doi: 10.1007/s12599-024-00914-2.

[18] J.H. Park, V.K. Madisetti, "CAPRI: A context-aware privacy framework for multi-agent generative AI applications," *IEEE Access*, vol. 13, pp. 43168–43177, 2025, doi: 10.1109/ACCESS.2025.3549312.

[19] F. Lorè, P. Basile, A. Appice, M. de Gemmis, D. Malerba, G. Semeraro, “An AI framework to support decisions on GDPR compliance,” *Journal of Intelligent Information Systems*, vol. 61, no. 2, pp. 541–568, 2023, doi: 10.1007/s10844-023-00782-4.

[20] D.J. Teece, G. Pisano, A. Shuen, “Dynamic capabilities and strategic management,” *Strategic Management Journal*, vol. 18, no. 7, pp. 509–533, 1997, doi: 10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

[21] K.M. Eisenhardt, J.A. Martin, “Dynamic capabilities: What are they?,” *Strategic Management Journal*, vol. 21, no. 10–11, pp. 1105–1121, 2000, doi: 10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E.

[22] D.J. Teece, “Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance,” *Strategic Management Journal*, vol. 28, no. 13, pp. 1319–1350, 2007, doi: 10.1002/smj.640.

[23] T. Birkstedt, M. Minkkinen, A. Tandon, 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.

[24] A. Batool, D. Zowghi, 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.

[25] O. Ismail, N. Ahmad, “Ethical and governance frameworks for artificial intelligence: A systematic literature review,” *International Journal of Interactive Mobile Technologies*, vol. 19, no. 14, pp. 121–136, 2025, doi: 10.3991/ijim.v19i14.56981.

[26] K. Bližnák, M. Munk, A. Pilková, “A systematic review of recent literature on data governance (2017–2023),” *IEEE Access*, vol. 12, pp. 149875–149888, 2024, doi: 10.1109/ACCESS.2024.3476373.

[27] M. Firdaus, H. T. Larasati, K-H. Rhee. “A blockchain-assisted distributed edge intelligence for privacy-preserving vehicular networks,” *Computers, Materials & Continua*, vol. 76, no. 3, pp. 2959–2978, 2023, doi: 10.32604/cmc.2023.039487.

[28] O. Rodríguez-Espíndola, S. Chowdhury, P.K. Dey, P. Albores, A. Emrouznejad, “Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing,” *Technological Forecasting and Social Change*, vol. 178, Art. no. 121562, 2022, doi: 10.1016/j.techfore.2022.121562.

[29] M. Wilbur, P. Pugliese, A. Laszka, A. Dubey, “Efficient data management for intelligent urban mobility systems,” in *Proceedings of the Workshop on Data-Driven and Intelligent Cyber-Physical Systems,* New York, NY: Association for Computing Machinery, 2021, pp. 22–26, doi: 10.1145/3459609.3460527.

[30] C. Basich, J. Svegliato, K.H. Wray, S. Witwicki, J. Biswas, S. Zilberstein, “Competence-aware systems,” *Artificial Intelligence*, vol. 316, Art. no. 103844, 2023, doi: 10.1016/j.artint.2022.103844.

[31] S.M. Narayan, N. Kohli, M.M. Martin, “Addressing contemporary threats in anonymised healthcare data using privacy engineering,” *npj Digital Medicine*, vol. 8, no. 1, Art. no. 145, 2025, doi: 10.1038/s41746-025-01520-6.

[32] H. Han, R.K. Shiwakoti, R. Jarvis, C. Mordi, D. Botchie, “Accounting and auditing with blockchain technology and artificial intelligence: A literature review,” *International Journal of Accounting Information Systems*, vol. 48, Art. no. 100598, 2023, doi: 10.1016/j.accinf.2022.100598.

[33] G. Rubeis, "Ethical implications of blockchain technology in biomedical research," *Ethik der Medizin*, vol. 36, no. 4, pp. 493–506, 2024, doi: 10.1007/s00481-024-00805-w.

[34] O. Amaral, S. Abualhaija, D. Torre, M. Sabetzadeh, L.C. Briand, "AI-enabled automation for completeness checking of privacy policies," *IEEE Transactions on Software Engineering*, vol. 48, no. 11, pp. 4647–4674, 2021, doi: 10.1109/TSE.2021.3124332.

[35] H. Chammaa, R. Ed-Daoudi, K. Benazzi, "Large language models for academic internal auditing," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1, pp. 687–694, 2025, doi: 10.14569/IJACSA.2025.0160166.

[36] D. Torre, S. Abualhaija, M. Sabetzadeh, L. Briand, K. Baetens, P. Goes, S. Forastier, "An AI-assisted approach for checking the completeness of privacy policies against GDPR," in *2020 IEEE 28th International Requirements Engineering Conference (RE)*, Piscataway, NJ: IEEE, 2020, pp. 136–146, doi: 10.1109/RE48521.2020.00025.

[37] J. Xu, "Leveraging LLaMA2 for improved document classification in English," *Peer Journal of Computer Science*, vol. 11, Art. no. e2740, 2025, doi: 10.7717/peerj-cs.2740.

[38] R. Gebler, I. Reinecke, M. Sedlmayr, M. Goldammer, "Enhancing clinical data infrastructure for AI research: Comparative evaluation of data management architectures," *Journal of Medical Internet Research (JMIR)*, vol. 27, Art. no. e74976, 2025, doi: 10.2196/74976.

[39] T. Rana, I. Steccolini, E. Bracci, D.G. Mihret, "Performance auditing in the public sector: A systematic literature review and future research avenues," *Financial Accountability & Management*, vol. 38, no. 3, pp. 337–359, 2022, doi: 10.1111/faam.12312.

[40] Y.-F. Wang, Y.-C. Chen, S.-Y. Chien, P.-J. Wang, "Citizens' trust in AI-enabled government systems," *Information Polity*, vol. 29, no. 3, pp. 293–312, 2024, doi: 10.3233/IP-230065.

[41] A. Sigfrids, M. Nieminen, J. Leikas, P. Pikkuaho, "How should public administrations foster the ethical development and use of artificial intelligence? A review of proposals for developing governance of AI," *Frontiers in Human Dynamics*, vol. 4, Art. no. 858108, 2022, doi: 10.3389/fhumd.2022.858108.

[42] B. Kuehnert, R. Kim, J. Forlizzi, H. Heidari, "The 'who', 'what', and 'how' of responsible AI governance: A systematic review and meta-analysis of (actor, stage)-specific tools," in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, New York, NY: Association for Computing Machinery, 2025, pp. 2991–3005, doi: 10.1145/3715275.3732191.

[43] H. Bleher, M. Braun, "Diffused responsibility: Attributions of responsibility in the use of AI-driven clinical decision support systems," *AI Ethics*, vol. 2, no. 4, pp. 747–761, 2022, doi: 10.1007/s43681-022-00135-x.

[44] A. Sriharan, N. Sekercioglu, C. Mitchell, S. Senkaiahliyan, A. Hertelendy, T. Porter, J. Banaszak-Holl, "Leadership for AI transformation in health care organization: Scoping review," *Journal of Medical Internet Research*, vol. 26, p. e54556, 2024, doi: 10.2196/54556.

[45] M.S. Al Jasem, T. De Clark, A.K. Shrestha, "Toward decentralized intelligence: A systematic literature review of blockchain-enabled AI systems," *Information*, vol. 16, no. 9, Art. no. 765, 2025, doi: 10.3390/info16090765.

[46] D. Leocádio, L. Malheiro, J.C.G. dos Reis, "Auditors in the digital age: A systematic literature review," *Digital Transformation and Society*, vol. 4, no. 1, pp. 5–20, 2025, doi: 10.1108/DTS-02-2024-0014.

[47] T.K.F. Chiu, Z. Ahmad, M. Ismailov, I.T. Sanusi, "What are artificial intelligence literacy and competency? A comprehensive framework to support them," *Computers and Education Open*, vol. 6, Art. no. 100171, 2024, doi: 10.1016/j.caeo.2024.100171.

[48] P. Suanpang, P. Pothipassa, "Integrating generative AI and IoT for sustainable smart tourism destinations," *Sustainability*, vol. 16, no. 17, Art. no. 7435, 2024, doi: 10.3390/su16177435.

[49] P. Tsarouhas, K. Grigoriadis, "A socio-technical framework for AI trust in public administration," *Transforming Government: People, Process and Policy,* vol. 20, no. 3, pp. 485–506, 2026, doi: 10.1108/TG-06-2025-0157.

[50] J. Schneider, R. Abraham, C. Meske, J. Vom Brocke, "Artificial intelligence governance for businesses," *Information Systems Management*, vol. 40, no. 3, pp. 229–249, 2023, doi: 10.1080/10580530.2022.2085825.

[51] F. Borgesano, A. De Maio, P. Laghi, R. Musmanno, "Artificial intelligence and justice: A systematic literature review and future research perspectives on Justice 5.0," *European Journal of Innovation Management*, vol. 28, no. 11, pp. 349–385, 2025, doi: 10.1108/EJIM-01-2025-0117.

[52] Y.A. Bena Y.A. Bena, R. Ibrahim, J. Mahmood, A. Al-Dhaqm, A. Alshammari, et al., "Big data governance challenges arising from data generated by intelligent systems technologies: A systematic literature review," *IEEE Access*, vol. 13, pp. 12859–12888, 2025, doi: 10.1109/ACCESS.2025.3528941.

[53] Á. Vaya-Arboledas, M. Ferrer-Oliva, J.A. Medina-Merodio, "Evolution and perspectives in IT governance: A systematic literature review," *Computers*, vol. 14, no. 12, Art. no. 520, 2025, doi: 10.3390/computers14120520.

[54] B. Kitchenham, O.P. Brereton, D. Budgen, M. Turner, J. Bailey, S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Information and Software Technology*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[55] B. Kitchenham, D. Budgen, P. Brereton, *Evidence-Based Software Engineering and Systematic Reviews.* Boca Raton, FL: CRC Press, 2015.

[56] B. Kitchenham, S. Charters, *Guidelines for performing systematic literature reviews in software engineering*, 2007.

[57] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *British Medical Journal*, vol. 372, Art. no. n71, 2021, doi: 10.1136/bmj.n71.

[58] T. Dybå, T. Dingsøyr, "Empirical studies of agile software development: A systematic review," *Information and Software Technology*, vol. 50, no. 9–10, pp. 833–859, 2008.

[59] A. Rohunen, P. Rodriguez, P. Kuvaja, L. Krzanik, J. Markkula, "Approaches to agile adoption," in *Product-Focused Software Process Improvement: 11th International Conference, PROFES 2010*, M. Ali Babar, M. Vierimaa, and M. Oivo, Eds. in Lecture

Notes in Computer Science, vol. 6156. Berlin/Heidelberg: Springer, 2010, pp. 77–91, doi: 10.1007/978-3-642-13792-1_8.

[60] M. Usman, E. Mendes, F. Weidt, R. Britto, "Effort estimation in agile software development: A systematic literature review," in *PROMISE '14: Proceedings of the 10th International Conference on Predictive Models in Software Engineering*, New York, NY, USA: Association for Computing Machinery, 2014, pp. 82–91, doi: 10.1145/2639490.2639503.

[61] Z.M. Altukhi, S. Pradhan, N. Aljohani, "A systematic literature review of the latest advancements in XAI," *Technologies*, vol. 13, no. 3, Art. no. 93, 2025, doi: 10.3390/technologies13030093.

[62] M. Gusenbauer, N.R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources," *Research Synthesis Methods*, vol. 11, no. 2, pp. 181–217, 2020, doi: 10.1002/jrsm.1378.

[63] V.C. Kaelin, M. Valizadeh, Z. Salgado, J.G. Sim, D. Anaby et al., "Capturing and operationalizing participation in pediatric re/habilitation research using artificial intelligence: A scoping review," *Frontiers in Rehabilitation Sciences*, vol. 3, Art. no. 855240, 2022, doi: 10.3389/fresc.2022.855240.

[64] E.J. Sacoto-Cabrera, A. Perez-Torres, L. Tello-Oquendo, M. Cerrada, "IoT, AI, and digital twins in smart cities: A systematic review for a thematic mapping and research agenda," *Smart Cities*, vol. 8, no. 5, Art. no. 175, 2025, doi: 10.3390/smartcities8050175.

[65] A. Tadesse Bogale, K.L. Debela, "Organizational culture: A systematic review," *Cogent Business & Management*, vol. 11, no. 1, Art. no. 2340129, 2024, doi: 10.1080/23311975.2024.2340129.

[66] J.R. Landis, G.G. Koch, "The measurement of observer agreement for categorical data," *Biometrics*, vol. 33, no. 1, pp. 159–174, 1977, doi: 10.2307/2529310.

[67] V. Braun, V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.

[68] M. Saunders, P. Lewis, A. Thornhill, *Research methods for Business Students*, 7th ed. Harlow: Pearson Education, 2016.

[69] P. Saunders, A. Huynh, J. Goodman-Delahunty, "Defining workplace bullying behaviour professional lay definitions of workplace bullying," *International Journal of Law and Psychiatry*, vol. 30, no. 4–5, pp. 340–354, 2007, doi: 10.1016/j.ijlp.2007.06.007.

[70] A. Abdelaziz, A.N. Mahmoud, "Data security in healthcare systems: Integration of information security and information management," *Journal of Cybersecurity and Information Management*, vol. 11, no. 2, pp. 17–26, 2023, doi: 10.54216/JCIM.110202.

[71] S. Xu, X. Yin, "Recommendation system for privacy-preserving education technologies," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, Art. no. 3502992, 2022, doi: 10.1155/2022/3502992.

[72] M. Zdravković, H. Panetto, G. Weichhart, "AI-enabled enterprise information systems for manufacturing," *Enterprise Information Systems*, vol. 16, no. 4, pp. 668–720, 2022, doi: 10.1080/17517575.2021.1941275.

[73] A. Choudhury, S. Elkefi, "Acceptance, initial trust formation, and human biases in artificial intelligence: Focus on clinicians," *Frontiers in Digital Health*, vol. 4, p. 966174, 2022, doi: 10.3389/fdgth.2022.966174.

[74] D. Schlegel, K. Schuler, J. Westenberger, "Failure factors of AI projects: Results from expert interviews," *International Journal of Information Systems and Project Management*, vol. 11, no. 3, pp. 25–40, 2023, doi: 10.12821/ijispm110302.

[75] D. Burema, N. Debowski-Weimann, A. von Janowski, J. Grabowski, M. Maftei et al., "A sector-based approach to AI ethics: Understanding ethical issues of AI-related incidents within their sectoral context," in *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*, New York, NY: Association for Computing Machinery, 2023, pp. 705–714, doi: 10.1145/3600211.3604680.

[76] J.W. Allen, B.D. Earp, J. Koplin, D. Wilkinson, "Consent-GPT: Is it ethical to delegate procedural consent to conversational AI?," *Journal of Medical Ethics*, vol. 50, no. 2, pp. 77–83, 2024, doi: 10.1136/jme-2023-109347.

[77] D.V. Osipov, "Ethics of AI technologies in 'sensitive' content creation and evaluation. School shooting cases," *Galactica Media: Journal of Media Studies*, vol. 6, no. 3, pp. 44–65, 2024, doi: 10.46539/gmd.v6i3.530.

[78] K. Chen, Z. Wang, B. Mi, "Private data protection with machine unlearning in contrastive learning networks," *Mathematics*, vol. 12, no. 24, Art. no. 4001, 2024, doi: 10.3390/math12244001.

[79] J. Paul, M.S.M.S. Annamalai, W. Ming, A. Al Badawi, B. Veeravalli, K.M.M. Aung, "Privacy-preserving collective learning with homomorphic encryption," *IEEE Access*, vol. 9, pp. 132084–132096, 2021, doi: 10.1109/ACCESS.2021.3114581.

[80] I.Y. Tyukin, T. Tyukina, D.P. van Helden, Z. Zheng, E.M. Mirkes et al., "Coping with AI errors with provable guarantees," *Information Sciences (NY)*, vol. 678, Art. no. 120856, 2024, doi: 10.1016/j.ins.2024.120856.

[81] T.J. Loftus M.M. Ruppert, B. Shickel, T. Ozrazgat-Baslanti, J.A. Balch et al., "Federated learning for preserving data privacy in collaborative healthcare research," *Digital Health*, vol. 8, 2022, doi: 10.1177/20552076221134455.

[82] B. Tag, N. van Berkel, S. Verma, B.Z.H. Zhao, S. Berkovsky et al., "DDoD: Dual denial of decision attacks on human-AI teams," *IEEE Pervasive Computing*, vol. 22, no. 1, pp. 77–84, 2023, doi: 10.1109/MPRV.2022.3218773.

[83] M. Tatasciore, V. Bowden, S. Loft, "Do concurrent task demands impact the benefit of automation transparency?," *Applied Ergonomics*, vol. 110, Art. no. 104022, 2023, doi: 10.1016/j.apergo.2023.104022.

[84] M.A.P. Chamikara, P. Bertok, I. Khalil, D. Liu, S. Camtepe, "Privacy preserving face recognition utilizing differential privacy," *Computers & Security*, vol. 97, Art. no. 101951, 2020, doi: 10.1016/j.cose.2020.101951.

[85] K. Sprenkamp, J.D. Fernández, S. Eckhardt, L. Zavolokina, "Overcoming intergovernmental data sharing challenges with federated learning," *Data Policy*, vol. 6, Art. no. e27, 2024, doi: 10.1017/dap.2024.19.

[86] A. Kouroutakis, "Rule of law in the AI era: Addressing accountability, and the digital divide," *Discover Artificial Intelligence*, vol. 4, no. 1, pp. 1–11, 2024, doi: 10.1007/s44163-024-00191-8.

[87] Y. Liu, M. Zhang, D. Qi, Y. Zhang, "Understanding the role of learner engagement in determining MOOCs satisfaction: A self-determination theory perspective," *Interactive Learning Environments*, vol. 31, no. 9, pp. 6084–6098, 2023, doi: 10.1080/10494820.2022.2028853.

[88] G. Recupito, F. Pecorelli, G. Catolino, V. Lenarduzzi, D. Taibi et al., "Technical debt in AI-enabled systems: On the prevalence, severity, impact, and management strategies for code and architecture," *Journal of Systems and Software*, vol. 216, Art. no. 112151, 2024, doi: 10.1016/j.jss.2024.112151.

[89] K. Branting, B. Brown, C. Giannella, J. Van Guilder, J. Harrold et al., "Decision support for detecting sensitive text in government records: Anonymous submission," *Artificial Intelligence and Law*, vol. 33, no. 1, pp. 171–197, 2025, doi: 10.1007/s10506-023-09383-6.

[90] D. Saxena, I. Gupta, R. Gupta, A.K. Singh, X. Wen, "An AI-driven VM threat prediction model for multi-risks analysis-based cloud cybersecurity," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 11, pp. 6815–6827, 2023, doi: 10.1109/TSMC.2023.3288081.

[91] S. Grodal, J. Ha, E. Hood, M. Rajunov, "Between humans and machines: The social construction of the generative AI category," *Organization Theory*, vol. 5, no. 3, doi: 10.1177/26317877241275125.

[92] F. Van Daalen, L. Ippel, A. Dekker, I. Bermejo, "Privacy Preserving n-Party Scalar Product Protocol," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 4, pp. 1060–1066, 2023, doi: 10.1109/TPDS.2023.3238768.

[93] J. Zeiser, "Owning decisions: AI decision-support and the attributability-gap," *Science and Engineering Ethics*, vol. 30, no. 4, Art. no. 27, 2024, doi: 10.1007/s11948-024-00485-1.

[94] A.K. Rai, I. Sharma, C. Silcox, "Accountability, secrecy, and innovation in AI-enabled clinical decision software," *Journal of Law and the Biosciences*, vol. 7, no. 1, Art. no. lsaa077, 2020, doi: 10.1093/jlb/lsaa077.

[95] T. Zhou, J. Shen, S. Ji, Y. Ren, L. Yan, "Secure and intelligent energy data management scheme for smart IoT devices," *Wireless Communications and Mobile Computing*, vol. 2020, no. 1, Art. no. 8842885, 2020, doi: 10.1155/2020/8842885.

[96] L.A. Cox Jr, "Information structures for causally explainable decisions," *Entropy*, vol. 23, no. 5, Art. no. 601, 2021, doi: 10.3390/e23050601.

[97] O.A. Cejas, S. Abualhaija, L.C. Briand, "Compai: A tool for GDPR completeness checking of privacy policies using artificial intelligence," in *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering*, New York, NY: Association for Computing Machinery, 2024, pp. 2366–2369, doi: 10.1145/3691620.3695353.

[98] G. Heo, S.E. Whang, "Redactor: A data-centric and individualized defense against inference attacks," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2023, pp. 14874–14882, doi: 10.1609/aaai.v37i12.26737.

[99] A. Singh, H.S. Pannu, A. Malhi, "Explainable information retrieval using deep learning for medical images," *Computer Science and Information Systems*, vol. 19, no. 1, pp. 277–307, 2022, doi: 10.2298/csis201030049s.

[100] R.-I. Chang, C. Yang, T.-W. Hsu, "An automatic sensitive image search system with generative artificial intelligence to identify data leaks on Internet," *Electronics*, vol. 14, no. 11, Art. no. 2254, 2025, doi: 10.3390/electronics14112254.

[101] A. Šarčević, D. Pintar, M. Vranić, A. Krajna, "Cybersecurity knowledge extraction using xai," *Applied Sciences*, vol. 12, no. 17, Art. no. 8669, 2022, doi: 10.3390/app12178669.

[102] S.A. Akinola, "Capabilities and apparent implications of artificial intelligence (AI) adoption in Nigerian academic libraries," in *University Library at a New Stage of Social Communications Development. Conference Proceedings*, no. 8. Dnipro: Ukrainian State University of Science and Technologies, 2023, pp. 283–289, doi: 10.15802/unilib/2023_293813.

[103] M. Weber, M. Engert, N. Schaffer, J. Weking, H. Krcmar, "Organizational capabilities for AI implementation – Coping with inscrutability and data dependency in AI," *Information Systems Frontiers*, vol. 25, no. 4, pp. 1549–1569, 2023, doi: 10.1007/s10796-022-10297-y.

[104] K.V. Suhanda, A. Faza, "Evaluating IT governance capability in managing operational contracts under PSAK 72: A case study of PT. XYZ's government service division," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 3, pp. 912–925, 2024, doi: 10.32520/stmsi.v13i3.3420.

[105] R.F. Mubarak, M.I. Fianty, "Leveraging COBIT 2019 to implement IT governance in mineral mining company," *Journal of Information Systems and Informatics*, vol. 5, no. 3, pp. 1058–1071, 2023, doi: 10.51519/journalisi.v5i3.545.

[106] D. Sanjaya, M.I. Fianty, "Measurement of capability level using COBIT 5 framework (case study: PT Andalan Bunda Bijak)," *Ultima InfoSys: Jurnal Ilmu Sistem Informasi*, vol. 13, no. 2, pp. 68–76, 2022, doi: 10.31937/SI.V13I2.2749.

[107] S. Singh, "Examining higher education students' intention of adopting MOOCs: An empirical study," *International Journal of Human and Technology Interaction*, vol. 18, no. 1, pp. 1–18, 2022, doi: 10.4018/IJTHI.299358.

[108] S. Ghirmai, D. Mebrahtom, M. Aloqaily, M. Guizani, M. Debbah, "Self-sovereign identity for trust and interoperability in the metaverse," in *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, Piscataway, NJ: IEEE, 2022, pp. 2468–2475, doi: 10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00345.

[109] R. Ali, I.D. Connolly, O.Y. Tang, F.N. Mirza, B. Johnston et al., "Bridging the literacy gap for surgical consents: An AI-human expert collaborative approach," *npj Digital Medicine*, vol. 7, no. 1, Art. no. 63, 2024, doi: 10.1038/s41746-024-01039-2.

[110] Y. Dai, Z. Chen, J. Li, S. Heinecke, L. Sun, R. Xu, "Tackling data heterogeneity in federated learning with class prototypes," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2023, pp. 7314–7322, doi: 10.1609/aaai.v37i6.25891.

[111] Y. Han, L. Wang, D. He, "Differential privacy technology of big data information security based on ACA-DMLP," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 9, pp. 1–9, 2022, doi: 10.14569/IJACSA.2022.0130905.

[112] A. Kotal, L. Elluri, D. Gupta, V. Mandalapu, A. Joshi, "Privacy-preserving data sharing in agriculture: Enforcing policy rules for secure and confidential data synthesis," in *2023 IEEE International Conference on Big Data (BigData),* Piscataway, NJ: IEEE, 2023, pp. 5519–5528, doi: 10.1109/BigData59044.2023.10386276.

[113] P. Nong, "Demonstrating trustworthiness to patients in data-driven health care," *Hastings Center Report*, vol. 53, pp. S69–S75, 2023, doi: 10.1002/hast.1526.

[114] P. Robinson, "Moral disagreement and artificial intelligence," in *AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society,* New York, NY: Association for Computing Machinery, 2021, p. 209, doi: 10.1145/3461702.3462534.

[115] M. von Zahn, S. Feuerriegel, N. Kuehl, "The cost of fairness in AI: Evidence from e-commerce," *Business & Information Systems Engineering*, vol. 64, no. 3, pp. 335–348, 2022, doi: 10.1007/s12599-021-00716-w.

[116] Y. Xiang, D. Luo, H. Xu, "Privacy-preserved evolutionary graph modeling via Gromov-Wasserstein autoregression," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2023, pp. 14566–14574, doi: 10.1609/aaai.v37i12.26703.

[117] M. Somasundaram, K.A.M. Junaid, S. Mangadu, "Artificial intelligence (AI) enabled intelligent quality management system (IQMS) for personalized learning path," *Procedia Computer Science*, vol. 172, pp. 438–442, 2020, doi: 10.1016/j.procs.2020.05.096.

[118] Z. Wang Y. Xu, J. Liu, Z. Li, Z. Li et al., "An efficient data sharing scheme for privacy protection based on blockchain and edge intelligence in 6G-VANET," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Art. no. 5031112, 2022, doi: 10.1155/2022/5031112.

[119] J. Zhang, "Multiple roles of big data platform and artificial intelligence architecture," in *Applied Mathematics, Modeling and Computer Simulation: Proceedings of the 3rd International Conference*, C.-H. Chen, A. Scapellato, A. Barbiero, and D. G. Korzun, Eds. in Advances in Transdisciplinary Engineering, vol. 42, Amsterdam: IOS Press, 2024, pp. 985–993, doi: 10.3233/ATDE231039.

[120] L. Cheng, K.R. Varshney, H. Liu, "Socially responsible AI algorithms: Issues, purposes, and challenges," *Journal of Artificial Intelligence Research*, vol. 71, pp. 1137–1181, 2021, doi: 10.1613/jair.1.12814.

[121] Y. Dai, A. Liu, C.P. Lim, "Reconceptualizing ChatGPT and generative AI as a student-driven innovation in higher education," *Procedia CIRP*, vol. 119, pp. 84–90, 2023, doi: 10.1016/j.procir.2023.05.002.

[122] R. Liu, S. Gupta, P. Patel, "The application of the principles of responsible AI on social media marketing for digital health," *Information Systems Frontiers*, vol. 25, no. 6, pp. 2275–2299, 2023, doi: 10.1007/s10796-021-10191-z.

[123] Y. Wang, J. Liu, M. Luo, L. Yang, L. Wang, "Privacy-preserving face recognition in the frequency domain," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022, pp. 2558–2566, doi: 10.1609/aaai.v36i3.20157.

[124] J. Zhang, Z. Zhang, "Ethics and governance of trustworthy medical artificial intelligence," *BMC Medical Informatics and Decision-Making*, vol. 23, no. 1, Art. no. 7, 2023, doi: 10.1186/s12911-023-02103-9.

Supplementary Materials

Full study-to-theme mapping based on revised reference numbering.

Table S1. IG functions.

Theme	References
Accountability and transparency	[1, 3, 5, 7, 9, 11, 12, 14–18, 27–29, 32, 33, 35–37, 70–72, 74–78, 80–83, 85, 86, 88, 89, 91–95, 97, 100, 102, 103, 108–116]
Data quality and integrity	[2, 5, 6, 8–11, 13–16, 18, 19, 27–29, 31, 32, 35, 36, 42, 70, 72–74, 76–81, 84–86, 88–90, 93, 96–103, 108, 109, 111, 112, 115–119]
Ethical governance and privacy	[1, 4, 6, 8, 13, 15, 17, 19, 29, 31, 32, 42, 71, 73, 75, 81, 82, 84, 90–92, 95–97, 99, 102, 113, 117–123]
Compliance and audit assurance	[3, 4, 30, 82, 83, 101, 114, 122, 123]
Security and risk management	[10, 12, 30, 33, 98]

Table S2. AI technologies supporting information governance.

Theme	References
Federated learning and data heterogeneity	[1, 4, 6, 8, 9, 12–14, 17, 18, 27, 29–31, 33, 36, 42, 70, 73, 74, 76–82, 84, 85, 89, 90, 92–94, 96, 99, 101–103, 108, 113, 114, 116–118, 120, 122, 123]
Ethical and responsible AI design	[2, 3, 7, 8, 10, 12–14, 16, 18, 30, 31, 33, 37, 71, 72, 75, 77, 80, 82, 83, 86, 88, 91, 94, 95, 97, 101–103, 111, 112, 117, 118, 120–122]
AI–blockchain integration for traceability and IP protection	[1–3, 5, 11, 15, 19, 28, 29, 32, 42, 72, 86, 95, 98, 100, 109–111, 124]
Machine learning (ML) for anomaly and fraud detection	[5, 6, 9, 11, 15, 28, 36, 75, 78, 89, 90, 92, 108, 112, 124]
Deep learning for Information extraction and leak detection	[19, 35, 70, 93, 96, 100, 114]
AI for risk assessment and security	[16, 17, 76, 79, 97, 109]

Table S3. Human roles and responsibilities in AI-driven governance systems.

Theme	References
Ethical and governance oversight	[1–9, 11–17, 19, 27–31, 33, 35–37, 42, 70–86, 88–103, 108, 109, 111–114, 116–118, 122, 123]
Technical development and validation	[1–6, 8–14, 16, 18, 19, 27, 29, 31–33, 36, 42, 70, 72–74, 77–81, 83–86, 89–99, 102, 103, 108, 109, 111–118, 120–124]
Policy and regulatory frameworks	[1–6, 8–14, 16, 18, 19, 27, 29, 31–33, 36, 42, 70, 72–74, 77–81, 83–86, 89–99, 102, 103, 108, 109, 111–118, 120–124]
Quality assurance and traceability	[2, 6, 8, 11, 14, 15, 18, 19, 30, 31, 37, 71, 75, 76, 78, 80, 86, 94, 98, 102, 109, 115, 118, 120, 121]
System design and workflow integration	[9, 17, 19, 28, 32, 70, 73, 79, 83–85, 89, 99–101, 111]

Table S4. Competencies and skill sets within the AI-enabled information governance (IG) domain.

Theme	References
Ethical and governance literacy	[5, 10, 17, 19, 27, 36, 42, 73, 74, 76, 91, 97, 100]
Collaborative and legal awareness	[5, 6, 12, 15–19, 27, 28, 34, 36, 37, 42, 71, 73, 74, 76, 78, 79, 86, 91, 98, 100–102, 109, 111, 124]
Technical and analytical proficiency	[1, 5–8, 12, 15–17, 19, 27, 28, 34, 36, 71–74, 76, 79–81, 88, 89, 95, 98, 99, 101–103, 111, 115, 116, 118, 120–122, 124]
Experimental and evaluation skills	[2, 6, 7, 12, 14–16, 28, 30, 33, 34, 70, 71, 74, 77–79, 81, 82, 89, 93, 101, 102, 111]
Human-centred and socio-technical competence	[3, 5, 6, 11, 12, 15–17, 28, 30, 71, 72, 75, 78, 79, 86, 96, 98, 101–103, 108, 111, 122, 124]