

DOI: https://doi.org/10.48009/1_iis_2026_116

AI privacy risk integration across project lifecycles: A systematic review

Hajar Niroomand, *Dakota State University*, Hajar.niroomand@trojans.dsu.edu

Abeer Alkhwaldi, *Dakota State University*, abeer.alkhwaldi@dsu.edu

Cherie Noteboom, *Dakota State University*, Cherie.Noteboom@dsu.edu

Abstract

AI-enabled tools are increasingly embedded in project environments, introducing privacy risks that remain conceptually underdeveloped as a structured risk domain. Although research examines AI applications in project management, the treatment of privacy risk within AI-enabled projects remains fragmented. This study conducts a systematic literature review of seventeen studies to critically map the conceptual gaps in privacy risk management across AI-enabled project contexts. Following established SLR guidelines, the review analyzes the literature through the lens of PMBOK® Guide's Risk Performance Domain and Contingency Theory to examine how AI-related privacy risks are conceptualized and integrated across predictive, adaptive, and hybrid project lifecycles. The findings reveal that current AI implementation research is structurally blind to project lifecycle governance, with fifteen of seventeen studies failing to link privacy risk to any lifecycle structure. The study introduces the APRIL framework (AI Privacy Risk Integration Across Project Lifecycles) as a proposed governance architecture to address this gap and outlines directions for future empirical research.

Keywords: Artificial Intelligence (AI), PMBOK® Guide, APRIL Framework (AI Privacy Risk Integration Across Project Lifecycles), project management, privacy risk

Introduction

Artificial intelligence (AI) is increasingly embedded in project environments, transforming how projects are planned, executed, and monitored (Niroomand & Noteboom, 2025). AI-enabled tools support decision-making, automate project analytics, and enhance forecasting across a range of domains including software development, construction, and digital transformation initiatives. While these technologies improve project performance and operational efficiency, they also introduce new privacy risks. AI systems frequently rely on large and heterogeneous datasets that may contain sensitive organizational, stakeholder, or personal information. Consequently, AI-enabled project tools may expose projects to privacy risks such as unintended data inference, model leakage, cross-system exposure, and re-identification of sensitive data.

Despite the rapid integration of AI into project environments, privacy risk is rarely treated as a structured project risk domain. Existing research tends to examine AI adoption, AI ethics, cybersecurity, or regulatory compliance in isolation, while relatively few studies explicitly address privacy risk management within the context of AI-enabled projects. As a result, privacy considerations are often treated as secondary compliance issues rather than as an integral component of project risk governance. This fragmentation

creates a gap in both theory and practice, leaving project managers without clear guidance on how privacy risks should be integrated into project risk management processes.

To critically map this gap, this study conducts a systematic literature review (SLR) examining the extent to which privacy risks are conceptualized and managed within AI-enabled project environments. The review documents the structural absence of lifecycle-based privacy risk governance across project management domains.

The study introduces the APRIL framework (AI Privacy Risk Integration Across Project Lifecycles) as a proposed governance architecture that establishes the conceptual space needed to reveal where the field falls short. The review is guided by the following research questions (RQs):

RQ1: How are privacy risks conceptualized in AI-enabled project environments?

RQ2: How are these risks integrated across predictive, adaptive, and hybrid project lifecycles?

RQ3: What risk management approaches are proposed, and what gaps remain in the literature?

Theoretical Foundation

PMBOK® Guide - Risk Performance Domain

The PMBOK® Guide emphasizes risk management as a continuous governance process encompassing risk identification, assessment, response, and monitoring throughout the project lifecycle (Project Management Institute, 2025). In AI-enabled projects, privacy risks may arise at multiple stages of project implementation due to the use of data-intensive technologies, algorithmic decision-making systems, and external AI services. Integrating privacy risk management into project governance therefore requires aligning privacy considerations with existing project risk management processes. Projects may follow different lifecycle structures (predictive, adaptive, or hybrid) depending on project characteristics and uncertainty levels. Predictive lifecycles rely on upfront planning in stable environments, adaptive lifecycles support iterative development in dynamic contexts, and hybrid lifecycles combine both. Because these structures manage uncertainty differently, privacy risk management practices may vary depending on the lifecycle adopted by an AI-enabled project.

Contingency Theory

Contingency theory provides a useful lens for understanding how governance mechanisms should adapt to contextual conditions. The theory suggests that organizational effectiveness depends on aligning structures and practices with environmental conditions such as technological complexity, uncertainty, and organizational context (*Donaldson, 2006*). In project management environments, lifecycle approaches can be viewed as contingency responses to different levels of uncertainty and project complexity. Applying contingency theory to AI-enabled projects suggests that privacy risk management strategies should be aligned with the lifecycle structure and the technological characteristics of AI systems deployed in the project environment.

Conceptual Framework

This study introduces the APRIL framework (AI Privacy Risk Integration Across Project Lifecycles) as a proposed governance architecture for integrating privacy risk management into AI-enabled project environments. The framework does not describe existing practice; it establishes the conceptual space needed to reveal where the field falls short and to guide future research toward structured privacy risk governance. The framework is anchored in three lifecycle types (predictive, adaptive, and hybrid) each

representing a distinct governance context that shapes how privacy risks should be identified and addressed. Within these lifecycles, AI systems introduce privacy risk emergence domains, including data exposure during collection, third-party processing risks, model inference and reconstruction attacks, re-identification of anonymized data, algorithmic opacity, retraining vulnerabilities, and consent misalignment.

These risks should be addressed through four interconnected processes aligned with the PMBOK® Guide's Risk Performance Domain: risk identification, assessment, response, and monitoring, operating as a continuous governance cycle. Two contextual factors moderate this process: lifecycle type, which shapes the approach to risk identification and mitigation, and the regulatory environment, which influences the rigor of risk assessment.

Together, as illustrated in Figure 1, these components define the governance architecture that current AI-enabled project management literature has yet to adopt.

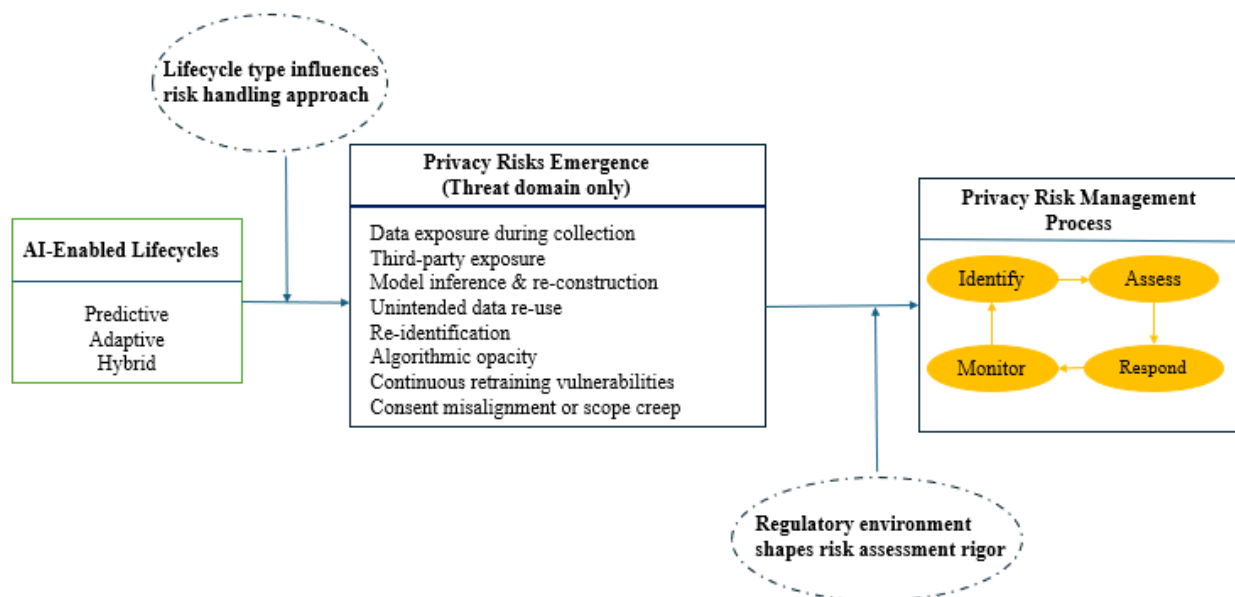


Figure 1. The APRIL Framework (AI Privacy Risk Integration Across Project Lifecycles)

Methodology

This study employs a systematic literature review (SLR) to synthesize research on privacy risk management in AI-enabled project environments. The review follows established SLR practices, combining PRISMA guidelines for transparent reporting (Liberati et al., 2009), the study selection protocol proposed by Kitchenham & Charters (2007), and the conceptual structuring approach of Webster & Watson (2002).

The study selection process followed PRISMA screening procedures, including title and abstract screening, full-text review, and backward citation snowballing. After removing duplicates and applying the inclusion and exclusion criteria, seventeen studies were retained for analysis. The full screening process is summarized in the PRISMA flow diagram (Figure 2). Studies focusing solely on general AI governance, cybersecurity, or regulatory discussions without reference to project or organizational implementation contexts were excluded.

Literature searches were conducted across Scopus, Web of Science, ABI/Inform, and the AIS eLibrary to identify studies addressing AI, privacy, and project environments. The search covered peer-reviewed publications between 2015 and 2026 and used combinations of keywords related to artificial intelligence, project management, privacy, and risk management (Table 1).

Table 1. Sources and Search String

Source	Search String
Scopus	("artificial intelligence" OR "AI-enabled" OR "AI-driven" OR "machine learning" OR "generative AI" OR "predictive analytics" OR "intelligent systems") AND ("project management" OR "project lifecycle" OR "project implementation" OR "project-based organization" OR "project environment" OR "program management" OR "SDLC" OR "software development lifecycle" OR "waterfall" OR "hybrid methodology" OR "IT project" OR "digital transformation project") AND (privacy OR "data protection" OR "personal data" OR "information privacy" OR "data exposure" OR "data security" OR "privacy threat" OR "data privacy" OR "information privacy" OR "privacy violation" OR "privacy harm" OR "privacy breach" OR "Privacy-by-design" OR "security by design"). LIMIT-TO: Language: English LIMIT-TO: Open Access Range: 2015-2026
AIS eLibrary	abstract:("artificial intelligence" OR "AI-enabled" OR "AI-driven" OR "machine learning" OR "generative AI" OR "predictive analytics" OR "intelligent systems") AND ("project management" OR "project lifecycle" OR "project implementation" OR "project-based organization" OR "project environment" OR "program management" OR "SDLC" OR "software development lifecycle" OR "waterfall" OR "hybrid methodology" OR "IT project" OR "digital transformation project") AND (privacy OR "data protection" OR "personal data" OR "information privacy" OR "data exposure" OR "privacy threat" OR "data privacy" OR "information privacy" OR "privacy violation" OR "privacy harm" OR "privacy breach" OR "Privacy-by-design"). Peer-reviewed only
Web of Science	abstract:("artificial intelligence" OR "AI-enabled" OR "AI-driven" OR "machine learning" OR "generative AI" OR "predictive analytics" OR "intelligent systems") AND ("project management" OR "project lifecycle" OR "project implementation" OR "project-based organization" OR "project environment" OR "program management" OR "SDLC" OR "software development lifecycle" OR "waterfall" OR "hybrid methodology" OR "IT project" OR "digital transformation project") AND (privacy OR "data protection" OR "personal data" OR "information privacy" OR "data exposure" OR "privacy threat" OR "data privacy" OR "information privacy" OR "privacy violation" OR "privacy harm" OR "privacy breach" OR "Privacy-by-design")
ABI/Inform	ABSTRACT(("artificial intelligence" OR "AI-enabled" OR "AI-driven" OR "machine learning" OR "generative AI" OR "agentic AI" OR AI OR LLM OR LTM) AND ("project management" OR "project lifecycle" OR "project-based" OR "project environment" OR "program management") AND (privacy OR "data protection" OR "privacy risk" OR "information privacy" OR "personal data" OR PII))

The selected studies were analyzed using a structured coding and data extraction protocol guided by the APRIL framework. For each paper, variables describing the AI context, project management context, privacy treatment, lifecycle integration, and risk management processes were recorded.

Coding examined how each study addressed privacy risk within AI-enabled project environments, including the presence of risk management processes aligned with the PMBOK® Guide, and whether privacy risk management was linked to predictive, adaptive, or hybrid project lifecycles. These variables enabled consistent comparison across studies and supported synthesis using the APRIL framework (Table 2).

Table 2. Data Extraction and Coding Variables

Variable used	Description	Analytical Purpose
AI Context	Type of AI technology discussed	Identifies technological setting where privacy risks emerge
Project Management Context	Domain in which AI is applied within project environment	Establishes relevance to AI-enabled PM
Privacy treatment	Whether discusses privacy/data governance or regulatory compliance	Supports analysis of privacy risk conceptualization (RQ1)
Lifecycle type	Whether study refers to predictive, adaptive, hybrid or not	Supports analysis of lifecycle integration (RQ2)
Risk process	Presence of risk management activities such as identification, assessment, mitigation, or monitoring of privacy risks.	Supports analysis of proposed risk management approaches (RQ3)
RQ1 contribution	Degree to which privacy risk is conceptually addressed	Used in synthesis of RQ1
RQ2 contribution	Degree to which privacy risk is linked to project lifecycle structures	Used in synthesis of RQ2
RQ3 contribution	Degree to which structured risk management approaches are proposed	Used in synthesis of RQ3

Quality Evaluation Strategy

A structured quality assessment protocol was applied to all seventeen studies across two independent dimensions, following established SLR practices (Kitchenham & Charters, 2007; Webster & Watson, 2002) (Table 3).

Table 3. Quality Assessment Framework

Dimension 1: Methodological quality		
M1	Clear research objectives	0:No objective stated, 1:Objectives implied or vague, 2: Objectives
M2	Transparent methodology	0:no method described, 1:no detail, 2:clearly described and replicable
M3	Theoretical grounding	0: No theoretical bases, 1: some theoretical bases, 2:Grounded in theory/framework
M4	Evidence strength	0: purely opinion, 1: partial evidence, 2: strong or systematic evidence
M5	Valid conclusion	0: unsupported, 1:partially supported, 2:fully supported
Dimension 2: Contribution to Research Questions		
RQ1	Conceptualization of privacy risk in AI-PM	0-2 – Not addresses, Mentioned, conceptualized
RQ2	Lifecycle Integration	0-2 – Not addresses, Implied, explicit lifecycle embedding
RQ3	Privacy risk management approaches	0-2 – none, general discussion, structured risk management model

Each paper was evaluated across two distinct dimensions. Dimension 1 assessed methodological quality with maximum score of 10 using five criteria: M1: clarity of research objectives; M2: transparency of research methods; M3: theoretical grounding; M4: strength of empirical or analytical evidence; M5: validity of conclusions relative to the presented evidence. Each criterion was scored on a three-point scale (0–2), producing a maximum possible methodological quality score of 10 per paper. Dimension 2 assessed RQ contribution with maximum score of 6, examining the extent to which each study addressed the review’s three research questions. Conceptualization of privacy risk in AI-enabled projects (RQ1), lifecycle integration of privacy considerations (RQ2), and approaches to privacy risk management (RQ3). The two

dimensions were evaluated and reported independently. Consistent with established SLR methodology, methodological quality appraisal must remain conceptually separate from thematic or research-question relevance (Kitchenham & Charters, 2007). Combining these measures risks conflating rigor with domain alignment and may compromise construct validity. Accordingly, methodological rigor was used to assess the trustworthiness of evidence, while RQ contribution informed analytical synthesis.

Overall, the quality assessment indicates moderate methodological rigor across the selected papers. Most studies clearly articulated their research objectives and conclusions, while methodological transparency varied depending on the study type. Empirical studies employing machine learning experiments or system evaluations tended to score higher on evidence strength (Aramali et al., 2025; Casillo et al., 2022; Herwanto et al., 2024; Kommusaar et al., 2026; Li et al., 2021; Sharma et al., 2024), whereas conceptual or literature-based discussions typically received lower scores on empirical validation (Adebayo et al., 2025; Assalaarachchi et al., 2025; Aziz, 2025; Galvez & Gürses, 2018; Ongbali et al., 2025; Raja, 2025; Yang et al., 2025). Mohamed, Al-Mhdawi, Ojiako, et al. (2025) represents an intermediate case, employing a systematic bibliometric analysis with quantitative multi-indicator evidence across nine databases.

Theoretical grounding was uneven across the corpus. Several studies relied primarily on technical or engineering approaches without explicit reference to broader theoretical frameworks related to project management, governance, or privacy risk. Only a small number of studies explicitly grounded their analyses in established frameworks: Kommusaar et al. (2026) drew on federated learning theory, GDPR governance instruments, and participatory research methodology; Aramali et al. (2025) applied the Technology Acceptance Model (TAM) as a formal theoretical foundation structuring both the research questions and the interpretation of findings; Sharma et al. (2024) applied NIST SP 800-30 R1 as a formal risk assessment methodology to derive likelihood and impact ratings.

In addition to quality and research-question contribution scoring, studies were categorized by relevance to the review topic. Papers directly addressing privacy risk governance in AI-enabled project environments were classified as primary relevance examples (Kommusaar et al., 2026; Yang et al., 2025), while studies providing supporting technical or contextual insights were classified as contextual relevance examples (Ongbali et al., 2025; Raja, 2025). Relevance classifications were applied independently of quality scores.

These results highlight an important characteristic of the emerging AI-project management literature: strong technical experimentation exists alongside conceptual discussions of ethics and governance, but relatively few studies integrate both rigorous empirical methods and explicit theoretical framing of privacy risk. While some studies demonstrated high technical rigor, their contribution to privacy risk governance in AI-enabled project environments was limited, reflecting the emerging and fragmented nature of the research area.

Results

The systematic search and screening process resulted in seventeen studies meeting the inclusion criteria for analysis. The study selection process followed PRISMA guidelines and is summarized in Figure 2. The search initially produced a larger pool of candidate studies across multiple databases. After removing duplicates and applying title and abstract screening, a smaller subset of studies was evaluated through full-text review. Additional relevant papers were identified through backward citation snowballing. The final corpus consists of seventeen studies addressing aspects of artificial intelligence, privacy, and project or organizational implementation contexts.

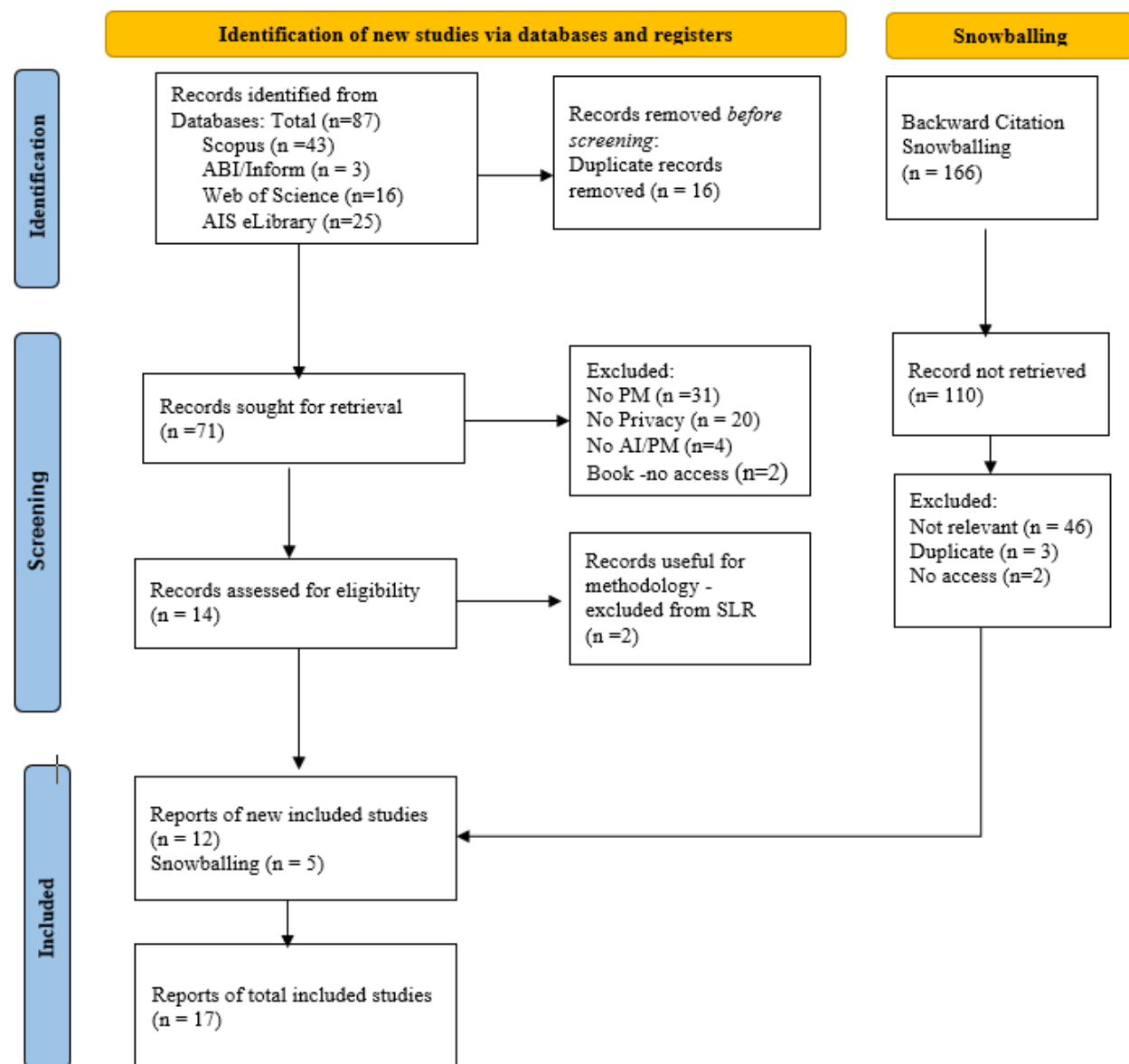


Figure 2. PRISMA Flow Diagram for Study Selection

Overall, the reviewed literature reflects a fragmented but emerging research area at the intersection of AI implementation, privacy risk, and project environments. While AI adoption in projects is widely discussed, explicit treatment of privacy risk as a structured project management concern remains limited.

Most studies approach privacy indirectly through discussions of data governance, regulatory compliance, or ethical AI deployment, rather than framing it as a dedicated project risk domain. In general project management contexts, privacy is treated primarily as an adoption barrier or governance concern (Ongbali et al., 2025; Raja, 2025). In construction, studies engage with privacy through data exposure (Li et al., 2021) and ethical dimensions (Adebayo et al., 2025; Yang et al., 2025), while others embed privacy within structured risk taxonomies linked to Gen AI integration in construction risk management (Liang et al., 2024; Mohamed, Al-Mhdawi, Ojiako, et al., 2025; Mohamed, Al-Mhdawi, Rahimian, et al., 2025). In software engineering contexts, Galvez & Gürses (2018) analyze the challenges that shifts in software engineering practice introduce into traditional threat modeling activities and their relationship to formal privacy goals,

while Abbas et al. (2025) and Assalaarachchi et al. (2025) address privacy as one concern within broader AI governance discussions. In several studies, privacy appears as one component of broader discussions of AI governance or data protection rather than as a distinct risk management construct within project environments (Aramali et al., 2025; Assalaarachchi et al., 2025; Aziz, 2025).

The literature is also dominated by review and conceptual studies (11/17), while empirically validated research remains relatively limited (6/17). Only six studies employ empirical evaluation methods such as system experiments, case analyses, or technical validation. Two of seventeen studies rely primarily on conceptual discussions (Galvez & Gürses, 2018; Yang et al., 2025), seven systematic literature reviews (e.g., Abbas et al., 2025; Adebayo et al., 2025), two non-systematic reviews (Ongbali et al., 2025; Raja, 2025), or analytical frameworks without empirical testing of proposed approaches. Aziz (2025) proposes a SWOT framework while examining Gen AI literature on the AEC (Architecture, Engineering, and Construction) industry. In contrast, Ongbali et al. (2025) provides a conceptual discussion of AI-enabled data acquisition and associated governance risks but does not include empirical validation.

Table 4 maps the reviewed studies to the key components of the APRIL framework. The table shows that while many studies address AI contexts and privacy-related concerns, explicit integration with project lifecycle structures is rarely specified, and risk processes are often limited to identification or general mitigation discussion. In the table, SDLC refers to Software Development Lifecycle, PII to Personally Identifiable Information, Gen AI to Generative AI, CNN to Convolutional Neural Network, AEC to Architecture, Engineering, and Construction, and NLP to Natural Language Processing.

Table 4. Mapping of Reviewed Studies to APRIL Framework

Paper	AI Context	Specific APRIL Domains	Risk Process	Lifecycle Type
(Abbas et al., 2025)	AI as a transformative force across SDLC.	Data exposure , third party exposure, retraining issues, Algorithmic opacity	Identification	Not specified (Discusses SDLC context)
(Adebayo et al., 2025)	AI in construction project management	Data quality and integration, lack of skill, ethical concern	General discussion	Not specified
(Aramali et al., 2025)	Gen AI (ChatGPT) in Project management	Data sharing with ChatGPT, data privacy	General discussion	Not specified
(Assalaarachchi et al., 2025)	AI /Gen AI is framed as an emerging assistive force in software project management	Data quality & exposure, lack of skilled project manager	Identification, Response / Mitigation	Not specified (Discusses SDLC / iterative context)
(Aziz, 2025)	Gen AI is framed as technological paradigm shift in AEC orgs.	Data exposure during collection (Gen AI), Data sharing	Identification, Assess (partial)	Not specified
(Casillo et al., 2022)	NLP techniques to extract and determine the presence/absence of privacy related works. CNN to identify PII	Data exposure in requirements, consent alignment or scope creep	Identification	Adaptive (Discusses SDLC / agile context)
(Galvez & Gürses, 2018)	Privacy threat modeling in software	Re-identification threat	Identification	Adaptive and Predictive (Also discusses SDLC)
(Herwanto et al., 2024)	NLP (privacy requirements Engineering)	Data quality & exposure (embedded in user stories)	Identification, Response / mitigation	Not specified (discusses SDLC context)

Paper	AI Context	Specific APRIL Domains	Risk Process	Lifecycle Type
(Kommusaar et al., 2026)	Federated Learning, AI implementation	Data exposure, re-identification in health data sharing risk/consent governance	Identification, Response (partial)	Not specified (roadmap FL development lifecycle context)
(Li et al., 2021)	Aggregating data issue by ML, Federated Learning as privacy preserving	Data exposure, third party access, re-identification risk	Identification and Response / mitigation	Not specified (technical implementation context)
(Liang et al., 2024)	AI ethics and robotics governance	Data exposure, algorithmic opacity	General Discussion	Not specified
(Mohamed, Al-Mhdawi, Ojiako, et al., 2025)	Gen AI/AI governance / risk framework	Data quality, third party exposure & legal risks, unintended exposure	Identification	Not specified
(Mohamed, Al-Mhdawi, Rahimian, et al., 2025)	Gen AI in construction risk mgmt.	Data exposure, third party exposure (Gen AI)	Identification / Mitigation-partial	Not specified
(Ongbali et al., 2025)	AI framed as a transformative tool for sustainable project planning and control	Data governance and ethical data collection, lack of technical skill	General discussion	Not specified
(Raja, 2025)	AI and ML can intervene throughout the project lifecycle	Data quality & exposure, lack of technical skill	Identification (partial, as barrier no risk assessment)	Not specified
(Sharma et al., 2024)	AI project risk and negative consequences	Data exposure/access, re-identification, information loss, black box/algorithmic opacity	Identification, assessment, Response / mitigation	Not specified
(Yang et al., 2025)	AI framed as a transformative but trust-challenged technology in construction	Onsite data collection risk, AI/algorithmic opacity concerns, unintended data use	Identification, Response (partial – not implemented)	Not specified

RQ1: Conceptualization of Privacy Risk

The first research question examined how privacy risks are conceptualized in AI-enabled project environments. The results indicate that privacy is rarely defined as a distinct analytical construct within the reviewed studies. Instead, privacy concerns are typically embedded within broader categories such as data security, information governance, or ethical AI considerations.

Several studies identify privacy-related threats associated with AI technologies, including data exposure during collection, third-party data sharing, model inference risks, and potential re-identification of sensitive data, in healthcare (Kommusaar et al., 2026), construction projects (Li et al., 2021), software development projects (Casillo et al., 2022), and agile requirements engineering (Herwanto et al., 2024). However, these risks are generally discussed as technical or compliance issues rather than as components of project risk management processes. Only a small number of studies explicitly frame privacy as a risk requiring structured identification and management within project environments (Herwanto et al., 2024; Kommusaar et al., 2026). Aramali et al. (2025), while examining ChatGPT adoption in project management, found that organizations currently respond to privacy risk through blunt instruments such as blocking Gen AI tools in firewalls or requiring approval with justification, reflecting reactive risk response in the absence of

structured assessment frameworks. Most of the six systematic review studies either identify privacy risk without further analysis, or treat it as a general governance concern, as is the case in Ongbali et al. (2025).

Among conceptual studies, Galvez & Gürses (2018) argue that privacy risk processes must become iterative and incremental rather than front-loaded, recognizing that lifecycle shifts from predictive to adaptive development fundamentally reconfigure how privacy threats are managed. By contrast, Raja (2025) treats privacy primarily as an adoption barrier, while Yang et al. (2025) embed it within a governance and design obligations framework rather than a project risk management process.

Overall, the findings suggest that privacy risk remains conceptually underdeveloped within AI-enabled project management literature, often conflated with cybersecurity or regulatory compliance rather than treated as a separate risk domain.

RQ2: Lifecycle Integration of Privacy Risk

The most significant finding of this review is that current AI-enabled project management research is structurally blind to project lifecycle governance. Of the seventeen studies reviewed, fifteen fail to explicitly link privacy risk to any project lifecycle structure, revealing a fundamental gap between how privacy risks are discussed in the literature and how they should be governed within project environments.

The structural reasons for this absence differ across disciplinary contexts. Studies in software engineering and AI system development reference software development lifecycles (SDLC) or iterative development environments rather than project management governance lifecycles (Assalaarachchi et al., 2025; Casillo et al., 2022; Herwanto et al., 2024). This reflects a disciplinary difference: software engineering research focuses on technical implementation artifacts and development process compliance, while project management governance operates at a higher organizational level concerned with risk, lifecycle phases, and stakeholder accountability. Casillo et al. (2022), for example, targets agile software development as its sole deployment context, treating user stories as a standard de facto notation in agile requirements engineering. As a result, privacy considerations are discussed within technical development processes but are not explicitly mapped across project management phases such as planning, execution, monitoring, and adaptation.

Construction studies (e.g., Aziz, 2025; Liang et al., 2024) implicitly adopt predictive lifecycle assumptions since construction project management is treated as a sequential, phase-gated process, but none explicitly frames privacy risk management within that lifecycle structure. Similarly, Aramali et al. (2025) uses the PMBOK® Guide predictive process group framework as its organizational structure, examining Gen AI applicability across Initiating, Planning, Executing, Monitoring and Controlling, and Closing phases, but does not mention the lifecycle structure. Only a limited number of studies address risk management frameworks that could potentially span project stages; however, even these studies do not explicitly integrate privacy risk management across project lifecycles (Mohamed, Al-Mhdawi, Rahimian, et al., 2025; Sharma et al., 2024).

This structural blindness to lifecycle governance is not incidental; it reflects the absence of an integrative framework that connects privacy risk to project lifecycle structures. The APRIL framework is introduced precisely to address this absence, providing the governance architecture that the reviewed literature has yet to adopt.

RQ3: Privacy Risk Management Approaches

The review identified several forms of privacy risk-related discussion across the literature. In relation to AI governance frameworks, Yang et al. (2025) proposed a 13-principle trustworthy AI framework derived from international regulations, Galvez & Gürses (2018) analyzed a three-paradigm privacy framework with

ten privacy goals mapped to threat modeling activities, Liang et al. (2024) identified nine ethical issue categories derived from established ethics frameworks, and Aziz (2025) proposed a SWOT framework addressing Gen AI governance risks in AEC organizations.

Studies related to data governance policies include Kommusaar et al. (2026), who discussed data-sharing agreements, role-based access, DPIA as a formal governance instrument, and risk registers maintained post-project; Yang et al. (2025), who emphasized privacy protection as a named design principle across the AI lifecycle; Aramali et al. (2025), who discussed organizational data privacy protocols, confidentiality policies, and the need for robust data governance frameworks; and Aziz (2025), who identified data governance as a critical issue requiring clear policies on data usage, storage, and disposal.

For ethical AI guidelines, proposals include privacy as a design obligation (Yang et al., 2025), ethical governance and algorithmic fairness (Ongbali et al., 2025), algorithmic ethics guidelines and regulatory impact assessments in construction AI (Adebayo et al., 2025), human-in-the-loop review and responsible use guidelines (Assalaarachchi et al., 2025), and AEC-specific ethical issue categories derived from EU ethics frameworks including ALTAI (Liang et al., 2024).

Studies addressing regulatory compliance mechanisms include those emphasizing GDPR and other regulatory instruments (Abbas et al., 2025; Kommusaar et al., 2026), legal risks including privacy breaches and data anonymization failures distributed across a quantitative risk taxonomy (Mohamed, Al-Mhdawi, Ojiako, et al., 2025), the absence of regulatory frameworks as a named risk factor alongside privacy breach and data retention risks (Mohamed, Al-Mhdawi, Rahimian, et al., 2025).

Fully structured privacy risk management models remain rare within the reviewed studies. Several studies propose technical solutions aimed at protecting privacy in AI-enabled systems, including federated learning architectures (Kommusaar et al., 2026; Li et al., 2021), automated privacy detection and requirements generation embedded in agile workflows (Herwanto et al., 2024), and transfer learning-based privacy disclosure detection in user stories (Casillo et al., 2022). Among these, Li et al. (2021) stands out for formally defining privacy, mathematically operationalizing it, and empirically evaluating the proposed architecture. Only two studies propose broader risk management frameworks that could support structured privacy risk handling in AI-enabled environments. Sharma et al. (2024) applies NIST SP 800-30 R1 to derive a twelve-factor risk model with likelihood and impact ratings and mapped controls. Mohamed, Al-Mhdawi, Rahimian, et al. (2025) proposes a structured framework of 25 risk factors across five categories with phase-specific mitigation strategies mapped to construction project lifecycle stages.

Herwanto et al. (2024) provides the most complete automated pipeline covering identification, assessment, response, and partial monitoring, and Casillo et al. (2022) embeds privacy detection within agile user story workflows. Both represent technical implementation tools rather than project lifecycle governance frameworks, reflecting the software engineering focus on development process compliance rather than organizational risk governance.

Consequently, the literature provides partial approaches to privacy risk mitigation but lacks integrated models that align privacy governance with project risk management processes.

Discussion

The findings highlight a significant conceptual and practical gap in the current literature on AI-enabled project environments. Although AI adoption in projects is widely discussed, privacy risks are rarely framed

as a core component of project risk governance. Instead, privacy concerns are typically addressed within broader discussions of cybersecurity, regulatory compliance, or ethical AI use, rather than as a dedicated project risk domain.

Within cybersecurity discussions, privacy violations are framed alongside data breaches and system security threats without being treated as a distinct governance concern (Aziz, 2025; Mohamed, Al-Mhdawi, Ojiako, et al., 2025). In regulatory compliance discussions, privacy appears primarily as a compliance obligation or adoption barrier, for example, as a jurisdictional barrier to AI adoption in construction (Adebayo et al., 2025), as a GDPR compliance requirement warranting anonymization and access controls (Abbas et al., 2025; Aramali et al., 2025), or as a regulatory obstacle to cross-organizational data sharing (Ongbali et al., 2025). Within ethical AI discussions, privacy is bundled alongside algorithmic bias, transparency, and accountability as one component of a broader responsible AI agenda (Assalaarachchi et al., 2025; Liang et al., 2024; Ongbali et al., 2025; Raja, 2025). Across all three framings, these studies acknowledge privacy concerns but situate them within governance or compliance contexts rather than within structured project risk management processes.

From a theoretical perspective, this fragmentation suggests that privacy risk has not yet been fully integrated into project management frameworks. The PMBOK® Guide's Risk Performance Domain emphasizes a holistic perspective on proactive risk management, stressing the importance of continuous risk identification, assessment, response, and monitoring throughout the project lifecycle (Project Management Institute, 2025). Yet the reviewed literature rarely connects privacy risks associated with AI systems to these established project risk management processes. Instead, most studies focus on technical privacy protections or AI governance mechanisms rather than on project risk management structures.

The absence of lifecycle-based analysis further reinforces this gap. Different project lifecycle structures (predictive, adaptive, and hybrid) introduce distinct governance mechanisms and risk management practices, yet existing research rarely examines how privacy risks evolve across project phases or how lifecycle structures influence privacy risk management strategies. Even studies proposing broader risk governance approaches tend to discuss risks at a general organizational level rather than linking them to specific project lifecycle stages (Mohamed, Al-Mhdawi, Rahimian, et al., 2025; Sharma et al., 2024).

Overall, while technical and governance discussions of AI privacy are increasing, the integration of privacy risk into project lifecycle governance remains underdeveloped. These findings support the need for a more integrated perspective that connects AI privacy risks, project lifecycle structures, and risk management processes, and point toward empirical validation of lifecycle-based privacy risk management models as a priority for future research.

Expected Contributions

This study contributes to research on AI-enabled project environments by critically mapping conceptual gaps in privacy risk management across AI-enabled project contexts. The review highlights that privacy is rarely treated as a structured project risk domain. The primary finding (fifteen of seventeen studies failed to link privacy risk to any project lifecycle structure) documents a fundamental structural blindness in current AI implementation research toward project lifecycle governance.

The study introduces the APRIL framework (AI Privacy Risk Integration Across Project Lifecycles) as a proposed governance architecture for future research and practice, providing the structural foundation that the reviewed literature has yet to adopt. Finally, the findings outline specific directions for future empirical

research, including lifecycle-based privacy risk governance models and organizational validation of the APRIL framework.

Future Research and Research Agenda

The findings suggest several directions for future research. Empirical studies are needed to examine how privacy risks emerge and are managed in real AI-enabled project environments, particularly across different industries. Future research should investigate how privacy risk management can be integrated across predictive, adaptive, and hybrid project lifecycles, including how lifecycle structures influence risk identification and mitigation strategies. Researchers should explore how privacy governance mechanisms can be aligned with project risk management processes, including the development and testing of lifecycle-based privacy risk frameworks.

Finally, empirical validation of the APRIL framework through case studies or organizational implementations would provide valuable insights into its practical applicability. Longitudinal studies tracking how privacy risks evolve across project phases, and action research studies co-developing privacy risk governance practices with project teams, would be particularly valuable in establishing the framework's utility across different project contexts and AI deployment scenarios.

Conclusions

The central finding of this systematic literature review is that current AI-enabled project management research is structurally blind to project lifecycle governance. Fifteen of seventeen studies failed to explicitly link privacy risk to any lifecycle structure, confirming that privacy is rarely treated as a structured project risk domain. Instead, existing research addresses privacy within broader discussions of cybersecurity, regulatory compliance, or ethical AI, reflecting fundamental fragmentation in the field.

Theoretically, project management theory has not yet been extended to address the distinctive privacy challenges introduced by AI systems. The APRIL framework (AI Privacy Risk Integration Across Project Lifecycles) is introduced as a proposed governance architecture providing a structural foundation for integrating privacy risk management into predictive, adaptive, and hybrid project lifecycles. APRIL is not a description of existing practice; it is a necessary future architecture that the reviewed literature has yet to adopt. In practice, project managers currently lack structured guidance for governing privacy risks in AI-enabled environments. The APRIL framework offers a starting point for developing lifecycle-aligned governance structures that systematically identify, assess, respond to, and monitor privacy risks.

This study has limitations that should be acknowledged. The APRIL framework has not yet been empirically validated and findings are drawn from an emerging and fragmented research area. Future research should prioritize empirical validation of lifecycle-based privacy risk governance models and organizational case studies testing the APRIL framework across different project lifecycle structures.

Acknowledgements

AI was used for editing assistance, including grammar checking and writing clarity. All intellectual content, framework development, and research contributions are the authors' original work.

References

- Abbas, T., Rathore, S. A., Turki, A., Khan, S., Alghushairy, O., & Daud, A. (2025). Enhancing Software Engineering With AI: Innovations, Challenges, and Future Directions. *IET Software*, 2025(1). <https://doi.org/10.1049/sfw2/5691460>
- Adebayo, Y., Udoh, P., Kamudyariwa, X. B., & Osobajo, O. A. (2025). Artificial Intelligence in Construction Project Management: A Structured Literature Review of Its Evolution in Application and Future Trends. *Digital*, 5(3). <https://doi.org/10.3390/digital5030026>
- Aramali, V., Cho, N., Pande, F., Al-Mhdawi, M. K. S., Ojiako, U., & Qazi, A. (2025). Generative AI in project management: Impacts on corporate values, employee perceptions, and organizational practices. *Project Leadership and Society*, 6, 100191. <https://doi.org/10.1016/j.plas.2025.100191>
- Assalaarachchi, L. I., Masood, Z., Hoda, R., & Grundy, J. (2025). Generative AI for Software Project Management: Insights from a Review of Software Practitioner Literature. *IEEE Software*. <https://doi.org/10.1109/MS.2025.3619936>
- Aziz, F. (2025). Generative Artificial Intelligence in AEC Organizations: A Literature and SWOT Analysis. *Journal of Intelligent Construction*, 3(3), 1–23. <https://doi.org/10.26599/JIC.2025.9180094>
- Casillo, F., Deufemia, V., & Gravino, C. (2022). Detecting privacy requirements from User Stories with NLP transfer learning models. *Information and Software Technology*, 146, 106853. <https://doi.org/10.1016/j.infsof.2022.106853>
- Donaldson, L. (2006). The Contingency Theory of Organizational Design: Challenges and Opportunities. In R. M. Burton, D. D. Håkansson, B. Eriksen, & C. C. Snow (Eds.), *Organization Design: The evolving state-of-the-art* (pp. 19–40). Springer US. https://doi.org/10.1007/0-387-34173-0_2
- Galvez, R., & Gürses, S. (2018). The Odyssey: Modeling Privacy Threats in a Brave New World. 2018 *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 87–94. <https://doi.org/10.1109/EuroSPW.2018.00018>
- Herwanto, G. B., Quirchmayr, G., & Tjoa, A. M. (2024). Leveraging NLP Techniques for Privacy Requirements Engineering in User Stories. *IEEE Access*, 12, 22167–22189. <https://doi.org/10.1109/ACCESS.2024.3364533>
- Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *Technical Report EBSE 2007-001*. Keele University and Durham University.
- Kommusaar, J., Elunurm, S., Chomutare, T., Kangasniemi, M., Salanterä, S., & Peltonen, L. (2026). A roadmap for federated learning projects using health data to guide sustainable artificial intelligence development in the European Union. *INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS*, 208. (WOS:001658279900001). <https://doi.org/10.1016/j.ijmedinf.2025.106242>
- Li, X., Chi, H., Lu, W., Xue, F., Zeng, J., & Li, C. Z. (2021). Federated transfer learning enabled smart work packaging for preserving personal image information of construction worker. *Automation in Construction*, 128, 103738. <https://doi.org/10.1016/j.autcon.2021.103738>

- Liang, C.-J., Le, T.-H., Ham, Y., Mantha, B. R. K., Cheng, M. H., & Lin, J. J. (2024). Ethics of artificial intelligence and robotics in the architecture, engineering, and construction industry. *Automation in Construction*, 162, 105369. <https://doi.org/10.1016/j.autcon.2024.105369>
- Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies. *Annals of Internal Medicine*, 151(4), 64–94.
- Mohamed, M. A. H., Al-Mhdawi, M. K. S., Ojiako, U., Dacre, N., Qazi, A., & Rahimian, F. (2025). Generative AI in construction risk management: A bibliometric analysis of the associated benefits and risks. *Urbanization, Sustainability and Society*, 2(1), 198–230. <https://doi.org/10.1108/USS-11-2024-0069>
- Mohamed, M. A. H., Al-Mhdawi, M. K. S., Rahimian, F. P., Ojiako, U., O'Connor, A., & Mahammed, C. (2025, March 24). Exploring the Risks of Integrating Generative Artificial Intelligence into Construction Risk Management: Insight from a Systematic Literature Review. *6th International Conference on Civil and Building Engineering Informatics*. <https://iccbei2025.hkust.edu.hk/>
- Niroomand, H., & Noteboom, C. B. (2025). Impact of Artificial Intelligence on Project Management Processes—A Systematic Review. *International Research Workshop on IT Project Management 2025*. 4. ICIS 2025. <https://aisel.aisnet.org/irwitpm2025/4>
- Ongbali, S. O., Egba, P., & Yekini, E. S. (2025). AI-Driven Sustainable Data Acquisition and Analysis in Project Planning and Control: A Critical Review. *NIPES - Journal of Science and Technology Research*, 7(1 Special Issue), 91–99. Scopus. <https://doi.org/10.37933/nipes/7.4.2025.SI12>
- Project Management Institute. (2025). *A guide to the project management body of knowledge (PMBOK guide—Eighth Edition)* (Eighth). Project Management Institute, Inc.
- Raja, V. (2025). Artificial Intelligence and Machine Learning in Project Management: A Conceptual Framework for Future Integration. *Journal of Business and Management Studies*, 7(5), 45–52. <https://doi.org/10.32996/jbms.2025.7.5.4>
- Sharma, M., Biros, D., Baham, C., & Biros, J. (2024). What Went Wrong? Identifying Risk Factors for Popular Negative Consequences in AI. *AIS Transactions on Human-Computer Interaction*, 16(2), 139–176. <https://doi.org/10.17705/1thci.00203>
- Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future. *MIS Quarterly*, 26(2), xiii–xxiii.
- Yang, L., Allen, G., Zhang, Z., & Zhao, Y. (2025). Achieving On-Site Trustworthy AI Implementation in the Construction Industry: A Framework Across the AI Lifecycle. *Buildings*, 15(1), 21. <https://doi.org/10.3390/buildings15010021>