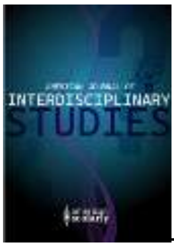


American Journal of Interdisciplinary Studies
Volume 03, Issue 01 (2022)
Page No: 01 – 30
eISSN: 3067-5146
Doi: 10.63125/caangg06

A SYSTEMATIC REVIEW OF LEGAL TECHNOLOGY ADOPTION IN CONTRACT MANAGEMENT, DATA GOVERNANCE, AND COMPLIANCE MONITORING

Md Nazrul Islam Khan[1];

[1] *Associate Lawyer, Yale Law Associate - Dhaka, Bangladesh*
Email: mkhan66@unh.newhaven.edu

ABSTRACT

This systematic review examines the adoption of legal technology within the interconnected domains of contract management, data governance, and compliance monitoring, with the aim of exploring how emerging digital innovations are reshaping legal workflows, improving operational efficiency, and strengthening risk management strategies. Drawing on evidence from 72 peer-reviewed journal articles and conference proceedings published between 2015 and 2022, the study integrates legal, technological, and organizational perspectives to provide a comprehensive understanding of current practices and trends. The synthesis identifies three central categories of technological application: (1) Contract Management—covering automation tools, AI-assisted contract review, natural language processing (NLP)–based clause extraction, and blockchain-enabled smart contracts, with an emphasis on their impact on drafting precision, negotiation speed, and full lifecycle management; (2) Data Governance—encompassing secure data storage, metadata management frameworks, privacy-preserving computation, and the integration of blockchain, advanced encryption, and identity management solutions to ensure regulatory compliance and data integrity; and (3) Compliance Monitoring—highlighting the use of AI, machine learning, predictive analytics, and real-time compliance dashboards to detect anomalies, flag violations, generate automated audit trails, and enable proactive policy enforcement. Findings reveal that legal technology adoption not only streamlines routine administrative functions but also facilitates predictive decision-making, enhances transparency, fosters cross-functional collaboration, and mitigates compliance risks. Nevertheless, implementation challenges such as system interoperability, integration costs, evolving data privacy regulations, and the requirement for continuous professional upskilling present persistent obstacles. This review offers a consolidated knowledge base for legal practitioners, policymakers, and researchers, underscoring critical success factors, identifying persistent research gaps, and outlining best practices for leveraging advanced digital tools to develop more agile, transparent, and resilient legal systems.

KEYWORDS

Legal technology, contract management, data governance, compliance monitoring, automation, AI, blockchain;

Citation:
Khan, M. N. I. (2022). A systematic review of legal technology adoption in contract management, data governance, and compliance monitoring. *American Journal of Interdisciplinary Studies,* 3(1), 1–30. https://doi.org/10.63125/caangg06

Received:
January 17, 2022

Revised:
February 20, 2022

Accepted:
March 16, 2022

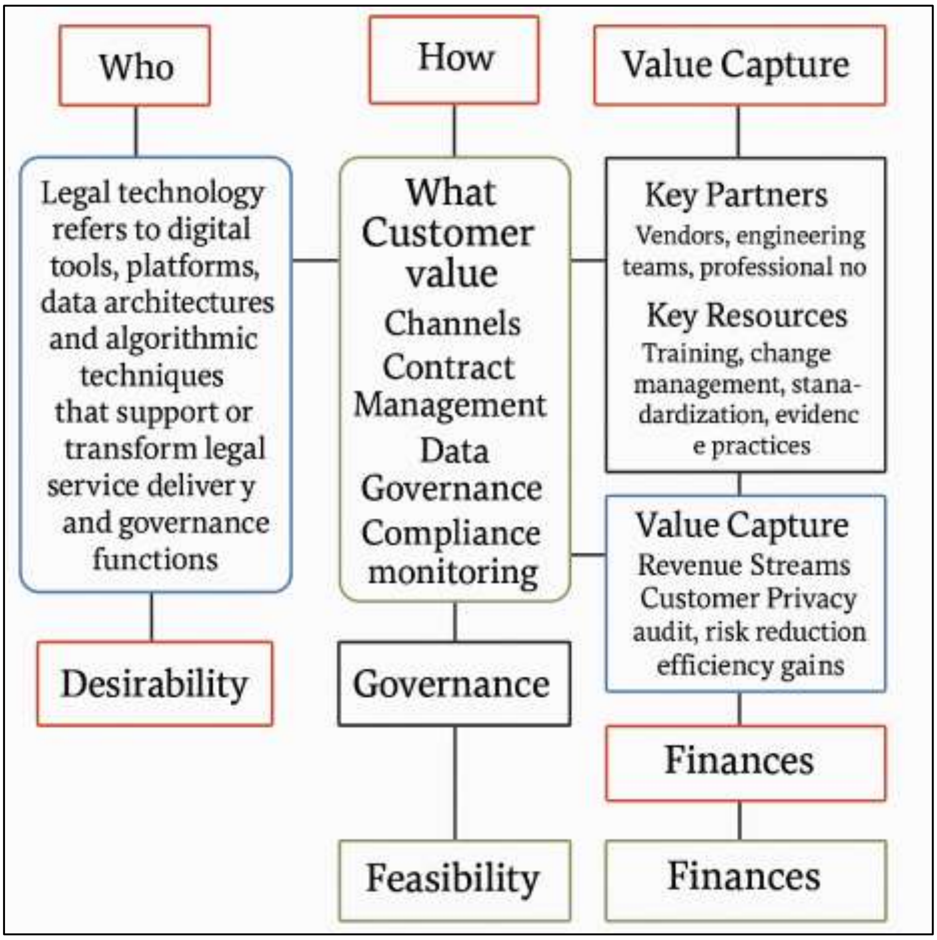
Published:
April 28, 2022

eISSN: 3067-5146
DOI:10.63125/caangg06

INTRODUCTION

The term "legal technology" refers to digital tools, platforms, data architectures, and algorithmic techniques that support or transform legal service delivery and governance functions across organizations (Corrales et al., 2019). Within this broad domain, contract management technology denotes software-enabled life-cycle controls for drafting, negotiation, approval, execution, performance tracking, renewal, and archival of agreements, often integrated with enterprise resource planning and customer relationship management systems. Data governance encompasses the policies, standards, metadata practices, and stewardship roles that organize data quality, lineage, and access rights across jurisdictions and business units. Compliance monitoring involves systematic procedures, audits, and controls for observing regulatory obligations, including privacy, financial reporting, anti-corruption, and sectoral rules, with escalation pathways and evidence trails (Fenwick et al., 2020). Together these domains define a socio-technical field in which law, information systems, and operations management intersect. Their convergence has created new possibilities for machine-readable contracts, structured clause repositories, automated review, risk scoring, and proof-of-compliance dashboards that align legal assurance with enterprise performance. Research identifies adoption as a multi-layer process conditioned by organizational capabilities, vendor ecosystems, and professional norms, making systematic synthesis necessary to clarify what implementation patterns emerge across contexts (Sanz & Zhu, 2021).

Figure 1: Legal Technology Adoption Framework Diagram


Who
How
Value Capture
Legal technology refers to digital tools, platforms, data architectures and algorithmic techniques that support or transform legal service deliver y and governance functions
What Customer value
Channels
Contract Management
Data Governance
Compliance monitoring
Key Partners
Vendors, engineering teams, professional no
Key Resources
Training, change management, stana-dardization, evidenc e practices
Value Capture
Revenue Streams
Customer Privacy
audit, risk reduction
efficiency gains
Desirability
Governance
Finances
Feasibility
Finances

International significance arises because contract portfolios, datasets, and regulatory exposures cross borders through global supply chains and digital markets. Multinational enterprises must operationalize obligations under frameworks such as the EU General Data Protection Regulation, the California Consumer Privacy Act, anti-money-laundering directives, and cross-border data transfer regimes, which impose documentation and auditability requirements directly addressable by legal technologies. Contract lifecycle management (CLM) platforms provide structured repositories and approval workflows that help align procurement, sales, and compliance teams across regions, while data governance catalogues and role-based access controls encode jurisdiction-specific limitations at the field or table level. In emerging markets, development agencies and regional authorities have advanced e-procurement and model contract initiatives that depend on interoperable templates and verifiable logs for donor compliance and anti-corruption safeguards (Donoghue, 2017). Sectoral regimes—pharma pharmacovigilance, medical device post-market surveillance, financial services conduct risk, and energy trading—require traceability across contract obligations and data flows, elevating the role of machine-assisted monitoring and defensible recordkeeping. Scholarly analyses point to the centrality of standardization, metadata models, and audit trails as the substrate of cross-jurisdictional compliance that legal technology can encode and surface.

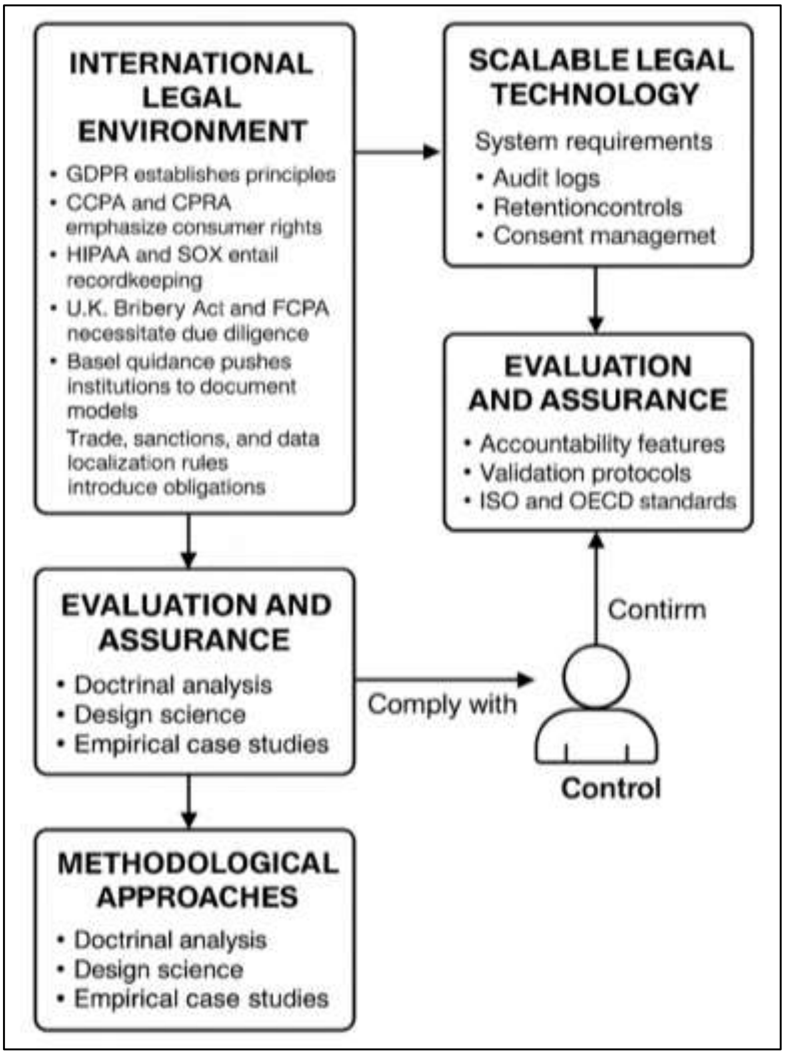
Foundational definitions also encompass the kinds of automation at stake. Document automation maps approved clause libraries into guided assembly, while natural language processing (NLP) systems perform entity extraction, clause classification, and obligation summarization to support review at scale (Zekos, 2021). Knowledge graphs represent relationships among parties, obligations, and regulatory references, enabling rule-based and probabilistic reasoning for change management when laws or policies are updated. Compliance analytics couple control catalogs with log data to provide key risk indicators and exceptions for internal audit, with frameworks like COSO, ISO 37301, and COBIT informing control design and assurance testing. Data governance platforms integrate data dictionaries, lineage maps, and stewardship workflows with legal taxonomies to encode legal bases for processing, retention schedules, and cross-border transfer restrictions. In contract management, digitized metadata—counterparty, governing law, termination rights, most-favored-nation clauses, data processing addenda—enables portfolio-level risk visibility and performance benchmarking across the enterprise (Raghupathi et al., 2018). Research threads from computer science, information systems, and socio-legal studies collectively describe how these techniques reshape routine legal work, reallocate expertise, and embed compliance within everyday business processes.

Adoption scholarship offers lenses for understanding uptake. Technology–Organization–Environment (TOE) and the Unified Theory of Acceptance and Use of Technology (UTAUT) emphasize compatibility with workflows, top-management support, vendor credibility, and regulatory pressure (Raghupathi et al., 2018). In professional settings, institutional logics and normative constraints shape acceptance alongside clear value propositions such as cycle-time reduction in contracting, improved audit readiness, and measurable error-rate reductions in document review. Empirical studies report that cross-functional governance bodies, including legal, compliance, IT security, procurement, and data officers, correlate with successful scale-up because they align taxonomies, controls, and change management. Implementation research further documents the role of training, explainability of algorithmic outputs, and defensible validation protocols in building trust within legal and audit teams (Pagallo et al., 2018). In the contract domain, studies associate template governance, negotiation playbooks, and deviation analytics with improved compliance to approved positions and more predictable outcomes. Across data governance and compliance monitoring, privacy-by-design patterns and data protection impact assessments integrate legal doctrine with engineering practice, showing how adoption proceeds when cross-disciplinary artifacts become routine.

The international legal environment frames the operational need for scalable technologies. GDPR establishes principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability, which translate into system requirements for audit logs, retention controls, and consent management . The CCPA and CPRA emphasize consumer rights and transparency, requiring data inventories and subject-access workflows, while sectoral rules such as HIPAA and SOX entail particular recordkeeping and attestation regimes (Butin & Le Métayer, 2015). Moreover, Anti-bribery frameworks like the U.K. Bribery Act and the U.S. Foreign Corrupt Practices Act necessitate third-party due diligence, contract clauses on representations and warranties, and monitoring controls integrated with vendor master data. Financial services operate under Basel operational risk and model risk guidance, pushing institutions to document models, validate outputs, and evidence control effectiveness, which interfaces with legal tech via automated evidence capture and defensible audit trails (Smallwood et al., 2012). Trade, sanctions, and data localization rules introduce obligations that organizations encode within contract terms and access policies, further elevating interoperability between legal, compliance, and data engineering systems.

Comparative studies show that heterogeneous enforcement intensities and regulatory interpretations across jurisdictions shape configuration choices in CLM, data catalogs, and monitoring dashboards.

Figure 2: International Legal Technology Control Framework


INTERNATIONAL LEGAL ENVIRONMENT
• GDPR establishes principles
• CCPA and CPRA emphasize consumer rights
• HIPAA and SOX entail recordkeeping
• U.K. Bribery Act and FCPA necessitate due diligence
• Basel quidance pushes institutions to document models
Trade, sanctions, and data localization rules introduce obligations
SCALABLE LEGAL TECHNOLOGY
System requirements
• Audit logs
• Retentioncontrols
• Consent managemet
EVALUATION AND ASSURANCE
• Accountability features
• Validation protocols
• ISO and OECD standards
EVALUATION AND ASSURANCE
• Doctrinal analysis
• Design science
• Empirical case studies
Comply with
Contirm
Control
METHODOLOGICAL APPROACHES
• Doctrinal analysis
• Design science
• Empirical case studies

Methodologically, the literature spans doctrinal analysis, design science, empirical case studies, surveys, and experimental evaluations. Doctrinal work articulates how legal principles map to technical requirements such as accountability, explainability, and data minimization, providing interpretive anchors for system design (Al-Abdullah et al., 2020). Design-science studies prototype rule languages, logic-based compliance engines, and machine-readable policy models to encode obligations and automate checks against transactional data. Empirical surveys in corporate legal departments report adoption drivers centered on contract cycle time, visibility, and self-service enablement for business users, alongside governance controls and audit readiness. Case studies examine integration with identity and access management, data warehouses, and enterprise messaging, noting that event-driven architectures support continuous controls monitoring that aligns with internal audit evidence needs. Experimental and benchmark-style evaluations in NLP for law document variable performance across clause extraction, classification, and entailment tasks, motivating curation of domain-specific corpora and annotation guidelines (Sype & Maalej, 2014). Interdisciplinary syntheses emphasize the co-evolution of legal doctrine, professional norms, and platform capabilities, highlighting how adoption patterns vary by industry structure and regulatory salience.

Within organizations, governance mechanisms link contract management, data governance, and compliance monitoring. Clause taxonomies and playbooks align with data dictionaries and retention schedules so that contractual promises and legal bases for processing are machine-linkable to data assets and control catalogs. Metrics such as time-to-signature, deviation rates from standard positions, and obligation completion rates interact with data quality scores, access exceptions, and control test pass rates to create integrated dashboards for management review and assurance. Change management covers template updates, policy revisions, and regulatory alerts, with knowledge graph or rules-engine layers propagating new requirements into contract clauses, data handling rules, and monitoring checks (Antignac et al., 2016; Subrato, 2018). Studies point to the importance of role clarity among legal operations, privacy officers, data stewards, and internal auditors so that ownership of artifacts and controls remains transparent across the life cycle. Cross-functional steering committees and architectural review boards provide escalation paths that connect legal interpretations to system configurations, enabling consistent application in geographically distributed teams and vendor networks. In sum, the literature defines a tightly coupled ecosystem where adoption in one domain conditions outcomes in the others through shared taxonomies, controls, and evidence practices.

Finally, scholarly attention converges on evaluation and assurance. Validation protocols for legal NLP include out-of-sample testing, human-in-the-loop review, and error taxonomy reporting to facilitate defensible use in high-stakes settings such as vendor diligence, sanctions screening, or privacy requests (Ara et al., 2022; Yeh, 2018). Auditability features—immutable logs, versioned templates, documented training data, and rationale capture for overrides—align with internal audit and regulator expectations and connect to enterprise risk management frameworks. International organizations and standards bodies document patterns for accountability and governance that inform organizational controls and procurement criteria, including ISO management systems, OECD guidelines for responsible business conduct, and FATF recommendations on beneficial ownership and transaction monitoring. Studies in organizational behavior highlight the role of learning loops, communities of practice, and professional identity in sustaining usage and data quality over time, pointing to the importance of building interpretive resources and shared artifacts that bridge legal and technical communities (Uddin et al., 2022; Li & Palanisamy, 2018). Comparative legal scholarship further clarifies how legal culture, judicial interpretation, and enforcement styles shape documentation and control emphases embedded in platforms, reinforcing the premise that adoption research benefits from cross-jurisdictional synthesis. Collectively, these strands establish the definitional scope, international salience, methodological approaches, and evaluative criteria that frame a systematic review of legal technology adoption in contract management, data governance, and compliance monitoring (Gazi, 2020; Akter & Ahad, 2022).

The primary objective of this systematic review is to synthesize and critically evaluate the existing scholarly and industry literature on the adoption of legal technology within three interrelated domains: contract management, data governance, and compliance monitoring. This entails mapping how organizations integrate technological solutions—such as contract lifecycle management (CLM) platforms, data governance frameworks, and compliance automation tools—into their operational and regulatory processes. By doing so, the review aims to clarify the definitional boundaries, functional overlaps, and interoperability challenges among these domains, offering an evidence-based framework for understanding how technological adoption enhances legal risk mitigation, operational efficiency, and regulatory adherence (Gazi, 2020; Arifur & Noor, 2022). A key component of this objective is to identify the factors that influence adoption, including organizational readiness, technological maturity, regulatory environment, and cross-functional governance structures, drawing from both theoretical lenses such as the Technology–Organization–Environment (TOE) framework and empirical adoption studies (Chen et al., 2012; Rahaman, 2022). Additionally, this review seeks to examine the international dimensions of legal technology adoption, recognizing that cross-border trade, multinational corporate structures, and jurisdictional regulatory diversity significantly shape technology implementation. This includes analyzing how global frameworks such as the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), U.K. Bribery Act, and Foreign Corrupt Practices Act (FCPA) inform the configuration of CLM clauses, metadata tagging in data governance systems, and audit trails in compliance monitoring tools. The review further aims to consolidate methodological approaches from doctrinal legal analysis, design science, empirical case studies, and experimental evaluations to ensure that insights are grounded in both normative legal principles and practical implementation outcomes (Hasan et al., 2022; Romanou, 2018). By integrating these perspectives, the overarching objective is to produce a comprehensive, cross-disciplinary synthesis that informs scholars, practitioners, and policymakers about the patterns, enablers, and constraints shaping the effective adoption of legal technology across diverse sectors and jurisdictions (Hossen & Atiqur, 2022; Simbeck, 2019).

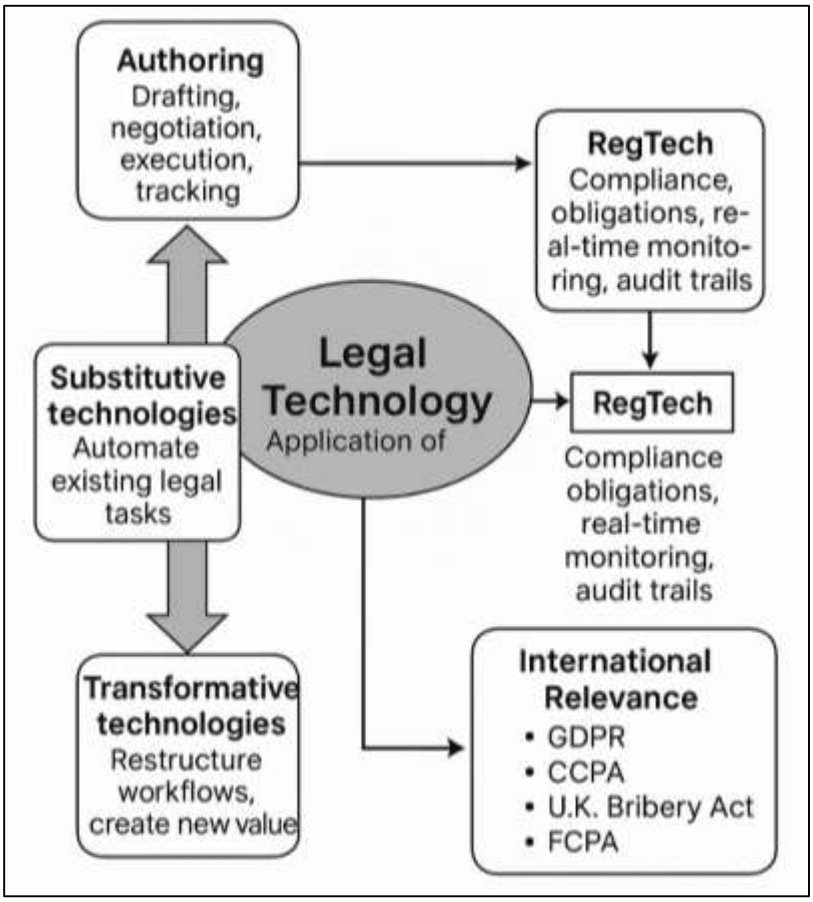
LITERATURE REVIEW

The literature surrounding legal technology adoption has grown exponentially over the past two decades, driven by the intersection of technological innovation, globalization, and the increasing complexity of regulatory frameworks. Legal technology, broadly defined, encompasses a wide range of digital tools, platforms, and algorithmic systems designed to enhance, automate, or transform legal service delivery, contractual processes, and compliance assurance. Within this expanding field, three domains—contract management, data governance, and compliance monitoring—have emerged as focal points for both academic inquiry and professional implementation. Each of these domains represents a distinct but interconnected set of practices that directly impact organizational efficiency, legal risk mitigation, and adherence to domestic and international regulations . Contract management has evolved from document storage to an integrated lifecycle process supported by Contract Lifecycle Management (CLM) platforms that offer template governance, clause libraries, AI-driven contract review, and portfolio analytics (Cheng et al., 2018). Data governance, traditionally a discipline within information systems, has expanded to include legal imperatives such as privacy-by-design, lawful basis mapping, and cross-border data transfer restrictions (Fernández-Caramés et al., 2019). Compliance monitoring, historically a manual audit and reporting process, now often leverages automation, continuous control monitoring, and predictive analytics to identify risks in real time. The existing literature spans doctrinal legal scholarship, design-science research, case studies, surveys, and experimental evaluations, each offering insights into different facets of technology adoption. However, while numerous studies address these domains in isolation, fewer works systematically explore their integration and the synergies that emerge when contract obligations, data governance rules, and compliance controls are technologically aligned. This review organizes the literature into thematic areas to examine definitional foundations, theoretical adoption models, domain-specific technological enablers, cross-sectoral comparisons, and implementation challenges (Zhu et al., 2019). The goal is to develop a structured synthesis that clarifies the patterns of adoption, identifies common success factors, and illuminates sector-specific nuances across different jurisdictions and organizational contexts.

Legal Technology in Contemporary Scholarship

Legal technology in contemporary scholarship is broadly conceptualized as the application of digital systems, software platforms, and algorithmic processes to support, automate, or transform legal and regulatory functions in organizations (Corrales et al., 2019). This domain spans a wide spectrum of solutions, from e-discovery platforms and contract lifecycle management (CLM) systems to compliance automation tools and AI-powered legal analytics. Contemporary research differentiates between “substitutive” technologies, which automate existing legal tasks, and “transformative” technologies, which restructure workflows and create new value propositions for legal services. In corporate legal operations, the adoption of such systems is often linked to measurable improvements in cycle time, cost efficiency, and risk visibility. Natural language processing (NLP) and machine learning (ML) have become central enablers, enabling automated contract review, clause classification, and predictive compliance analytics. Legal technology also encompasses regulatory technology (RegTech), which addresses compliance obligations through real-time monitoring, transaction screening, and audit trail generation (Sjöberg, 2019). Scholarly definitions consistently emphasize that legal technology is not merely a set of tools but a socio-technical construct—shaped by legal doctrine, organizational culture, and regulatory context—that redefines how legal expertise is delivered and embedded in business processes (Bues & Matthaei, 2016; Tawfiqul et al., 2022). This multidimensional nature means its study must incorporate perspectives from law, information systems, organizational theory, and innovation management to accurately capture the dynamics of adoption and integration.

Figure 3: Conceptualizing Legal Tehnology in Scholarly Research


Authoring
Drafting, negotiation, execution, tracking
RegTech
Compliance, obligations, re-al-time monito-ring, audit trails
Legal Technology
Application of
Substitutive technologies
Automate existing legal tasks
RegTech
Compliance obligations, real-time monitoring, audit trails
Transformative technologies
Restructure workflows, create new value
International Relevance
• GDPR
• CCPA
• U.K. Bribery Act
• FCPA

While contract management, data governance, and compliance monitoring are distinct disciplines, literature increasingly highlights their operational and conceptual interdependence. Contract management focuses on the structured administration of contractual relationships, encompassing drafting, negotiation, execution, and post-award performance tracking. Data governance, by contrast, is concerned with establishing policies, standards, and stewardship mechanisms to ensure data quality, lineage, and lawful use. Compliance monitoring involves systematic oversight to verify adherence to applicable laws, regulations, and internal policies, often using frameworks such as COSO or ISO 37301 for structuring control environments (Reduanul & Shoeb, 2022; Yeung, 2018). The boundaries between these areas blur in practice because contractual obligations often encode data governance requirements (e.g., privacy clauses, data localization stipulations), and compliance monitoring depends on both contractual records and data governance artifacts for evidence. Studies in enterprise systems integration show that siloed approaches lead to duplicated efforts, inconsistent interpretations, and heightened compliance risk. As a result, scholars argue for a more unified conceptualization in which legal, operational, and technical frameworks are interlinked through common taxonomies, metadata models, and governance processes (Howard et al., 2018; Reduanul & Shoeb, 2022). Understanding the distinctiveness of each domain remains essential for role clarity and accountability, but appreciating their interconnections is critical for designing effective, technology-enabled governance ecosystems.

Interoperability in legal technology refers to the ability of disparate systems—such as CLM platforms, data governance tools, and compliance monitoring solutions—to exchange, interpret, and act upon shared information seamlessly. Literature in information systems emphasizes that interoperability can be syntactic (data formats), semantic (shared meaning), or pragmatic. In legal contexts, this translates into mapping contract clause metadata to data governance policies and linking both to compliance control libraries (Sazzad & Islam, 2022; Taal et al., 2016). Research on "policy-as-code" and rule-based reasoning demonstrates how regulatory requirements can be codified in machine-executable formats, enabling automated compliance checks triggered by events in operational systems. Knowledge graphs are another enabler, capturing relationships among contractual terms, regulatory obligations, and data assets to facilitate integrated risk analysis. Empirical studies report that interoperability reduces audit preparation time, minimizes compliance gaps, and supports cross-functional collaboration by ensuring that legal interpretations are consistently embedded in technical configurations. However, achieving interoperability requires overcoming challenges in standards alignment, vendor integration capabilities, and organizational change management (Mohtaramzadeh et al., 2018; Sohel & Md, 2022). The literature underscores that integrated legal-technical systems are not merely a technological ambition but an operational necessity in environments where obligations, data flows, and controls are deeply interlinked.

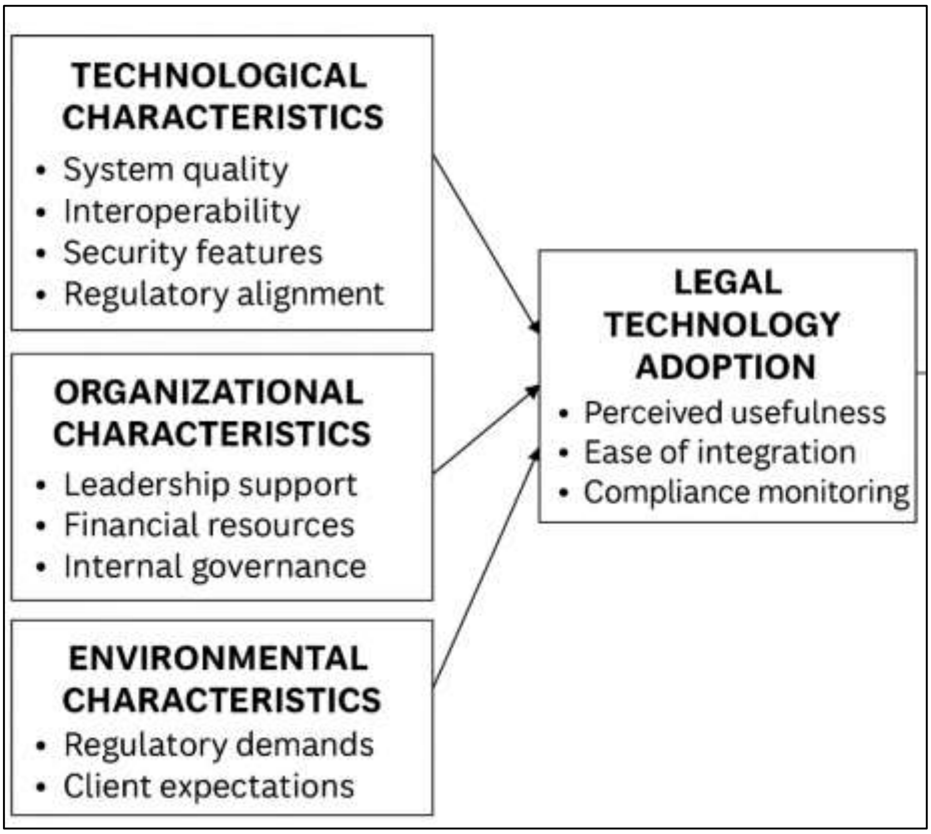
The international relevance of legal technology adoption arises from the globalization of commerce, supply chains, and data flows, which expose organizations to multi-jurisdictional regulatory regimes (Kabanda & Brown, 2017; Akter & Razzak, 2022). Frameworks such as the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the U.K. Bribery Act, and the U.S. Foreign Corrupt Practices Act (FCPA) impose diverse compliance obligations that must be operationalized through technological systems. For example, GDPR's principles of lawfulness, data minimization, and accountability require organizations to maintain verifiable data inventories, implement retention controls, and document consent mechanisms—features often embedded within data governance and compliance platforms. Similarly, anti-bribery and anti-money-laundering regimes necessitate third-party due diligence processes, contractual clauses on compliance warranties, and continuous monitoring of high-risk transactions. Literature on cross-border contracting highlights the role of CLM systems in managing multi-language templates, jurisdiction-specific clauses, and international arbitration provisions. Comparative studies show that differences in enforcement intensity, legal culture, and data localization requirements shape the configuration of technology systems in different regions. Sector-specific rules—such as HIPAA in healthcare, SOX in financial reporting, and FERC compliance in energy trading—further add layers of jurisdictional complexity (Ansong & Boateng, 2018). The convergence of these requirements underscores the necessity for legal technologies that can be configured to handle heterogeneous rule sets while maintaining consistent, auditable processes across global operations.

Frameworks for Technology Adoption

The Technology–Organization–Environment (TOE) framework offers a structured lens for understanding legal technology adoption by examining the interplay of technological readiness, organizational capacity, and environmental pressures.

In legal contexts, the technological dimension includes system quality, interoperability, security features, and alignment with regulatory requirements. Studies in corporate legal departments show that functionalities such as automated clause extraction, compliance monitoring dashboards, and metadata-driven contract repositories influence perceived usefulness and ease of integration (Cao et al., 2018). The organizational dimension captures leadership support, financial resources, and internal governance structures, which are pivotal in overcoming resistance to change in risk-averse legal environments. Empirical findings suggest that organizations with cross-functional governance bodies involving legal, compliance, IT, and procurement teams exhibit higher implementation success rates for contract lifecycle management (CLM) and data governance tools (Martins et al., 2019). The environmental dimension encompasses external regulatory demands, client expectations, and industry competition, which frequently act as catalysts for adoption. For example, GDPR compliance pressures have accelerated the integration of privacy-by-design features into enterprise data governance platforms. Comparative case studies indicate that multinational enterprises face amplified environmental drivers due to jurisdictional diversity, necessitating adaptable system configurations. Collectively, TOE-based analyses reveal that successful legal technology adoption hinges on balancing internal capacity with external demands, underscoring the framework's relevance for understanding adoption patterns in legal service environments (Mirkovski et al., 2016).

Figure 4: Legal Technology Adoption Framework Model



The Unified Theory of Acceptance and Use of Technology (UTAUT) framework identifies performance expectancy, effort expectancy, social influence, and facilitating conditions as key determinants of technology adoption. In legal services, performance expectancy often centers on perceived improvements in contract cycle times, error reduction in document review, and enhanced compliance visibility. Research indicates that when legal professionals recognize clear efficiency gains—such as reducing contract review times through AI-driven analytics—the likelihood of adoption increases significantly. Effort expectancy, or the perceived ease of use, is influenced by interface design, integration with existing workflows, and training availability. Studies show that user-friendly dashboards and guided contract assembly interfaces facilitate faster adoption among lawyers with varying technical proficiency (Ahmad et al., 2019). Social influence in legal contexts often emanates from senior partners, general counsel, or regulatory authorities endorsing specific tools, creating normative pressure for adoption. Facilitating conditions—including IT support, vendor responsiveness, and availability of legal-specific customizations—are critical to sustaining use over time. UTAUT-based studies in law firms and corporate legal departments also highlight moderating factors such as age, professional experience, and practice area, which shape adoption dynamics (Chao et al., 2016). Empirical evidence suggests that aligning system design with legal practitioners' cognitive workflows and risk management priorities increases both initial uptake and long-term utilization. This makes UTAUT a valuable lens for examining behavioral drivers in the adoption of legal technology.

Institutional theory examines how organizational behaviors are shaped by normative, coercive, and mimetic pressures, providing a rich framework for understanding legal technology uptake. Normative pressures in legal settings emerge from professional standards, ethical codes, and accreditation requirements, which can encourage or constrain the adoption of certain technologies (Mirkovski et al., 2019). For instance, compliance monitoring tools may be more readily adopted when they align with professional obligations for due diligence and recordkeeping. Coercive pressures stem from regulatory mandates, client demands, and contractual obligations that necessitate technological capabilities for evidencing compliance. These forces are particularly strong in sectors like finance and healthcare, where legal risk exposure is high and regulators mandate auditable digital systems (Alghamdi et al., 2018). Mimetic pressures involve organizations imitating the practices of industry leaders, often adopting similar CLM systems, data governance frameworks, or compliance automation platforms to maintain competitiveness. Literature shows that law firms and corporate legal departments frequently benchmark their technology adoption strategies against peers to attract clients and retain talent. Institutional theory also helps explain resistance to adoption when new technologies conflict with entrenched professional identities or challenge billable-hour models (Stella & Bwalya, 2018). By integrating these perspectives, scholars highlight that legal technology adoption is not purely a rational efficiency-driven process but is deeply embedded in social legitimacy, professional norms, and institutional conformity.

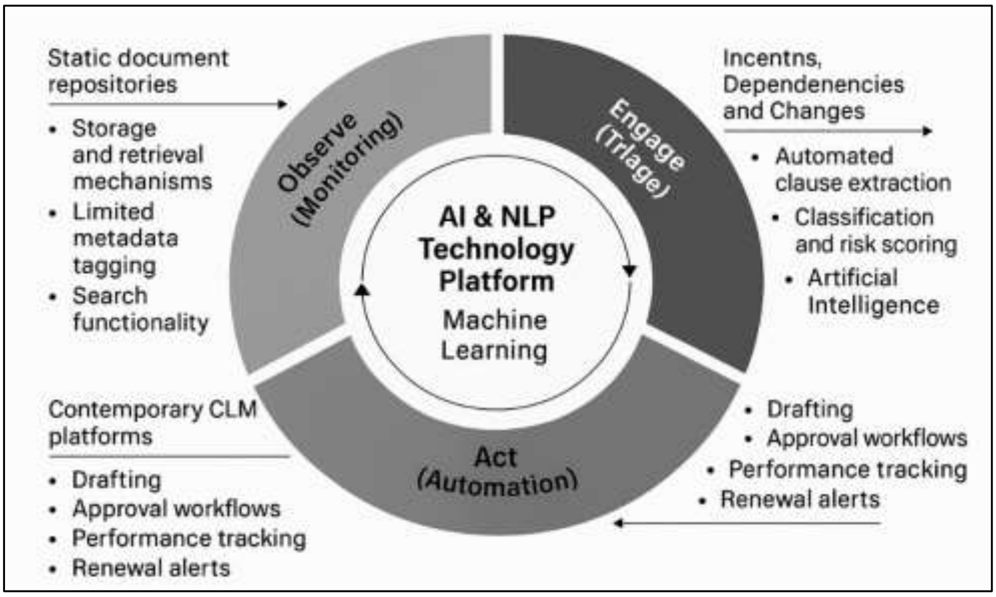
The socio-technical systems (STS) perspective emphasizes the interdependence of social and technical subsystems, positing that optimal outcomes in technology adoption occur when both are jointly optimized. In legal digitalization, this means aligning the technical design of platforms—such as CLM systems, data governance tools, and compliance monitoring dashboards—with the social realities of legal work, including professional culture, decision-making hierarchies, and collaborative workflows (Kompella, 2017). Literature in law and technology demonstrates that failure to address social dynamics, such as trust in algorithmic outputs or perceived threats to professional autonomy, can undermine even technically sound implementations. STS research shows that successful adoption requires participatory design processes involving end-users, governance committees, and compliance officers to ensure that systems reflect shared interpretations of legal requirements. Technical subsystems must also be configured to accommodate the interpretive flexibility inherent in legal reasoning, allowing for exceptions, annotations, and contextual overrides. The STS lens further underscores the importance of feedback loops—such as post-implementation reviews and continuous training—to adapt systems to evolving legal and organizational contexts (Krigsholm et al., 2020). Studies in multinational enterprises show that socio-technical alignment enhances not only adoption rates but also compliance accuracy and user satisfaction. By framing legal technology adoption as an ongoing negotiation between social actors and technical artifacts, the STS perspective provides a holistic understanding of the complexities and contingencies inherent in digital transformation within legal domains.

Contract Management Technology

The evolution of contract management technology reflects a transition from static document repositories to dynamic, end-to-end Contract Lifecycle Management (CLM) systems designed to optimize contractual processes across their full life cycle. Early digital solutions primarily served as storage and retrieval mechanisms, offering limited metadata tagging and search functionality. These repositories often existed in isolation from other enterprise systems, creating challenges in version control, obligation tracking, and cross-departmental visibility (Haraldson et al., 2020). Contemporary CLM platforms integrate drafting, automated approval workflows, electronic signatures, performance tracking, and renewal alerts, thereby enabling proactive management of contractual relationships. Studies highlight that CLM adoption improves contract cycle times, reduces administrative burden, and enhances compliance by embedding legal-approved templates and clause standards into business workflows. Integration with enterprise resource planning (ERP) and customer relationship management (CRM) systems further facilitates synchronization between contractual commitments and operational execution. Research also underscores that modern CLM systems support granular metadata capture—such as governing law, termination rights, and data processing obligations—allowing for advanced analytics and risk assessments (Li et al., 2018). The shift from passive storage to active contract intelligence marks a significant transformation in how organizations approach contractual governance, embedding it more deeply into the operational and compliance fabric of the enterprise.

Artificial Intelligence (AI) and Natural Language Processing (NLP) technologies have redefined contract analysis by enabling automated clause extraction, classification, and risk scoring at scale. Traditional manual review processes are resource-intensive, prone to human error, and often inconsistent in identifying contractual risks. NLP-driven tools can parse large volumes of contracts to identify key terms, obligations, and deviations from approved standards with high accuracy (Gibreel & Hong, 2017). These systems use pre-trained legal language models, pattern recognition, and machine learning classifiers to extract structured data from unstructured legal text. Risk scoring modules assess the likelihood and potential impact of contractual breaches or unfavorable terms, supporting decision-making in procurement, sales, and compliance functions. Empirical studies demonstrate that AI-assisted review reduces contract analysis time by up to 80%, freeing legal teams to focus on higher-value strategic work. Furthermore, integration with regulatory rule sets enables real-time compliance checks during contract drafting and negotiation, minimizing downstream legal exposure. Research also notes the importance of explainability in AI-driven legal tools, with human-in-the-loop validation processes ensuring defensibility in audits and disputes. The literature positions AI and NLP as essential enablers of contract intelligence, transforming reactive contract review into proactive risk and compliance management (Fors-Owczynik, 2016).

Figure 5: AI-Powered Contract Management Framework



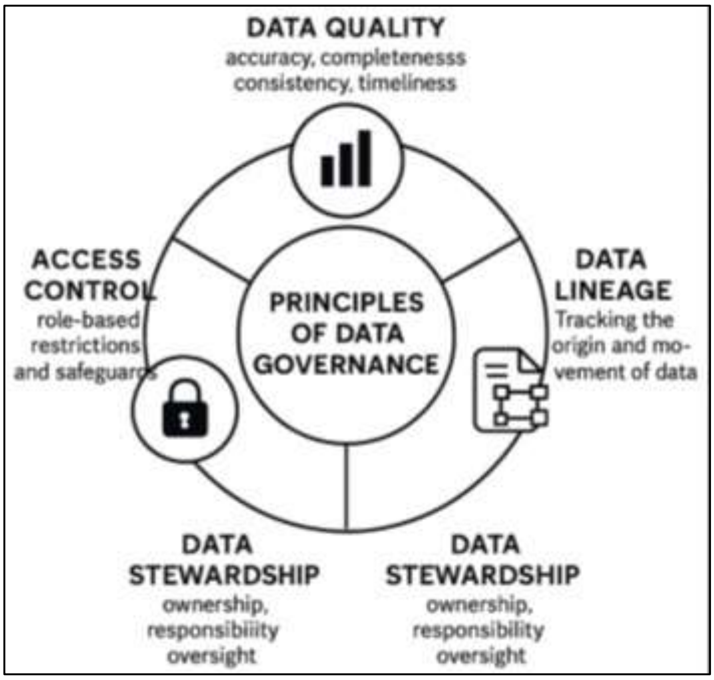
Data Governance Frameworks

Data governance is defined as the system of decision rights, accountabilities, and processes that ensure the effective management of data assets throughout their lifecycle. The literature identifies data quality as a foundational principle, encompassing dimensions such as accuracy, completeness, consistency, and timeliness. High-quality data underpins compliance with contractual obligations and regulatory reporting, reducing legal exposure from inaccurate disclosures. Data lineage refers to the ability to trace data flows from origin to consumption, providing transparency for audits, investigations, and regulatory submissions (Eigenstetter, 2020). Legal scholars emphasize lineage documentation as a key evidentiary tool for demonstrating lawful processing under regimes like the General Data Protection Regulation (GDPR). Data stewardship assigns responsibility to specific individuals or roles for maintaining data quality and ensuring compliance with policies. Effective stewardship links technical controls to legal requirements, such as retention limits and confidentiality classifications. Access control mechanisms enforce role-based permissions, safeguarding sensitive contractual and personal data from unauthorized use. Studies in regulated industries, including finance and healthcare, show that robust governance programs integrating these principles improve both operational efficiency and legal defensibility (Proskurina¹, 2019). Collectively, the literature positions these four principles as the structural pillars that align technical data management with legal compliance objectives, enabling organizations to manage risk proactively while maximizing data utility.

Privacy-by-Design (PbD) is a proactive framework that embeds privacy protections into systems, processes, and business practices from their inception. In legal contexts, PbD aligns with regulatory mandates such as Article 25 of the GDPR, which requires controllers to implement technical and organizational measures that integrate data protection principles into processing activities. Literature identifies legal basis mapping as a complementary practice, whereby each processing activity is explicitly tied to a lawful basis—such as consent, contractual necessity, or legitimate interest—documented for audit readiness (Sadok et al., 2020). This mapping ensures that data governance frameworks are directly linked to compliance obligations, reducing the risk of unauthorized or unlawful processing. Scholars note that legal basis mapping also facilitates Data Protection Impact

Assessments (DPIAs), which evaluate the risks of high-impact processing activities and identify mitigating controls. Empirical studies in multinational enterprises demonstrate that integrating PbD principles with automated metadata tagging in governance tools improves visibility over sensitive data categories and streamlines responses to regulatory inquiries (Pitt et al., 2018).

Figure 6: Principles of Effective Data Governance


DATA QUALITY
accuracy, completenesss consistency, timeliness
ACCESS CONTROL
role-based restrictions and safeguards
PRINCIPLES OF DATA GOVERNANCE
DATA LINEAGE
Tracking the origin and movement of data
DATA STEWARDSHIP
ownership, responsibiiity oversight
DATA STEWARDSHIP
ownership, responsibility oversight

In the healthcare sector, PbD has been applied to ensure HIPAA compliance by embedding role-based access, encryption, and audit logging into electronic health record systems. In financial services, it supports anti-money laundering controls by limiting data access to investigative personnel while maintaining traceability for regulators. The literature underscores that the combined application of Privacy-by-Design and legal basis mapping operationalizes legal principles into concrete, enforceable system behaviors, bridging the gap between policy and practice .

Cross-border data governance presents significant challenges due to the diversity of national and regional regulations governing data transfers and localization (Taylor, 2020). Under the GDPR, personal data may only be transferred outside the European Economic Area to jurisdictions with adequate protections or under approved mechanisms such as Standard Contractual Clauses (SCCs) (Badran, 2018). Similar restrictions appear in Brazil's LGPD, Singapore's PDPA, and China's PIPL, each imposing specific safeguards for international transfers. Data localization laws, present in countries such as Russia, India, and Indonesia, require certain categories of data—often financial or health-related—to be stored and processed within national borders. Literature highlights the operational complexity these rules create for multinational organizations, necessitating technical controls such as geo-fencing, jurisdiction-specific cloud hosting, and localized encryption key management (Tehrani et al., 2018). In contractual contexts, cross-border compliance is often addressed through jurisdiction-specific clauses, service-level agreements, and breach notification protocols. Studies indicate that failure to manage cross-border data flows effectively can lead to regulatory penalties, reputational damage, and operational disruptions. Industry-specific regulations further complicate the landscape—such as HIPAA's restrictions on international transmission of patient health information or financial regulators' requirements for local record-keeping (Liverani et al., 2018). The literature consistently calls for an integrated approach that combines legal expertise, data governance frameworks, and technical enforcement to navigate the intersecting demands of transfer compliance and localization mandates (Sullivan, 2019).

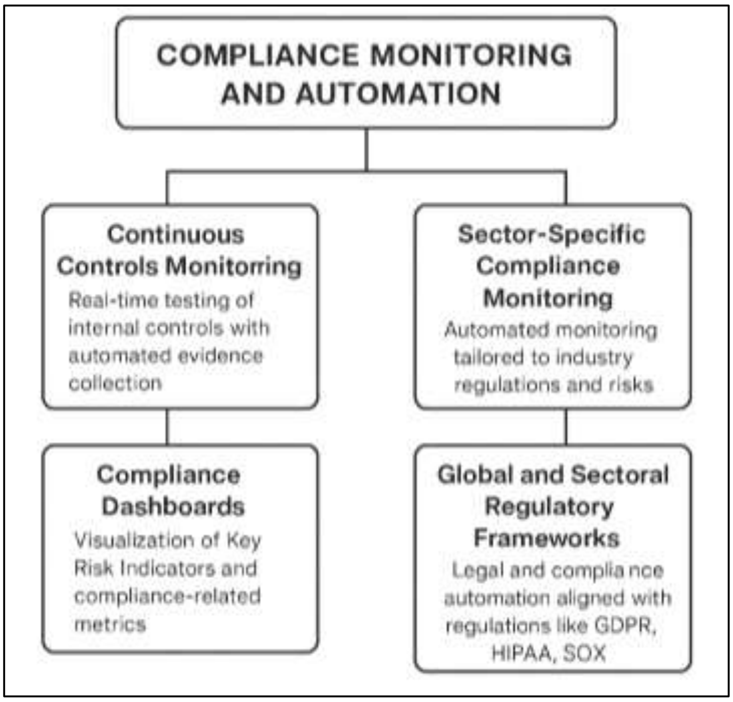
Compliance Monitoring and Automation

Continuous Controls Monitoring (CCM) refers to the use of technology to perform real-time or near real-time testing of internal controls, enabling organizations to detect anomalies, policy breaches,

eISSN: 3067-5146
DOI:10.63125/caangg06

and compliance gaps proactively . Literature in accounting and information systems highlights that CCM integrates data feeds from enterprise systems—such as ERP, CLM, and data governance platforms—to monitor transactions, user activities, and data flows against predefined control parameters (Adrot et al., 2017). Automated evidence collection is a complementary capability, ensuring that each control test is accompanied by immutable, timestamped records that can be presented to auditors or regulators. Studies in regulated sectors demonstrate that CCM reduces audit preparation time, enhances control coverage, and improves the timeliness of remediation efforts. By linking CCM outputs to contract clauses, privacy policies, and regulatory requirements, organizations can create a closed-loop compliance system where identified breaches automatically trigger investigations or workflow escalations. Research also emphasizes the role of machine learning in refining control parameters, allowing systems to adapt to emerging risk patterns and reduce false positives. Case studies in financial services and healthcare show that organizations leveraging CCM and automated evidence collection achieve higher audit pass rates and reduce the risk of regulatory penalties (Medeiros, 2019). Collectively, the literature frames CCM as a cornerstone of modern compliance automation, embedding assurance functions directly into operational workflows.

Figure 7: Overview of Compliance Monitoring and Automation


COMPLIANCE MONITORING AND AUTOMATION
Continuous Controls Monitoring
Real-time testing of internal controls with automated evidence collection
Sector-Specific Compliance Monitoring
Automated monitoring tailored to industry regulations and risks
Compliance Dashboards
Visualization of Key Risk Indicators and compliance-related metrics
Global and Sectoral Regulatory Frameworks
Legal and complia nce automation aligned with regulations like GDPR, HIPAA, SOX

Sector-specific compliance monitoring reflects the unique regulatory landscapes and operational risks inherent to industries such as finance, healthcare, energy, and pharmaceuticals. In finance, compliance frameworks such as the Basel Accords, the Dodd–Frank Act, and anti-money laundering (AML) directives mandate robust monitoring of transactions, model risk management, and capital adequacy reporting (Beach et al., 2020). Literature shows that financial institutions deploy automated surveillance systems to flag suspicious transactions, enforce sanctions screening, and monitor adherence to lending and investment limits. In healthcare, HIPAA and related privacy regulations require continuous monitoring of patient data access, breach detection, and compliance with security protocols. Automated systems in this sector integrate with electronic health record (EHR) platforms to enforce access controls, audit logs, and incident response workflows. In the energy sector, compliance monitoring addresses requirements from the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), focusing on operational reliability, market transparency, and cybersecurity (Elgammal et al., 2016). For pharmaceuticals, regulatory bodies such as the European Medicines Agency (EMA) and the U.S. Food and Drug Administration (FDA) enforce pharmacovigilance and good manufacturing practices. Studies demonstrate that sector-specific monitoring systems leverage domain-specific taxonomies, risk models, and audit templates to ensure alignment with specialized compliance requirements. Across all sectors, automation reduces manual workload, improves regulatory reporting accuracy, and enhances the capacity to respond swiftly to compliance breaches (Chernyaev et al., 2020).

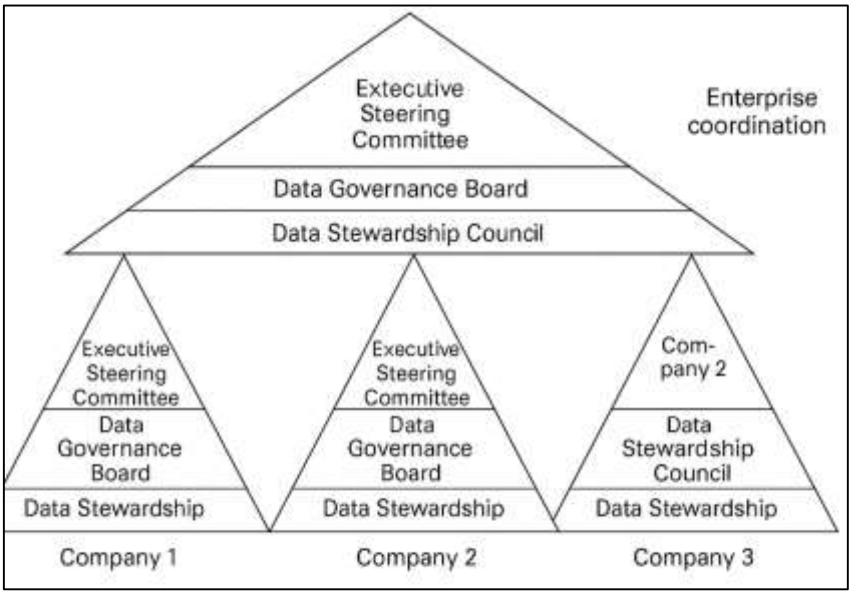
Global and sectoral regulatory frameworks are primary drivers of compliance automation, as their requirements increasingly demand granular, verifiable, and timely evidence of adherence. The GDPR mandates operationalization of principles such as lawfulness, transparency, and accountability, requiring organizations to maintain detailed records of processing activities and implement automated mechanisms for fulfilling data subject rights. HIPAA in the United States imposes stringent requirements for safeguarding protected health information, driving adoption of automated access monitoring, encryption, and breach notification systems in healthcare (Zhong et al., 2018). The Sarbanes–Oxley Act (SOX) enforces rigorous financial reporting controls, prompting the integration of CCM and automated evidence collection into corporate finance functions. Anti-Money Laundering (AML) directives from the Financial Action Task Force (FATF) and regional regulators require continuous transaction monitoring, sanctions screening, and suspicious activity reporting, all of which are enhanced by automation (Griggs et al., 2018). Literature shows that these frameworks not only mandate compliance but also shape the configuration of technology systems, including predefined control libraries, jurisdiction-specific workflows, and audit-ready reporting capabilities. Empirical research highlights that organizations aligning automation strategies with regulatory requirements achieve greater efficiency in audit processes, reduce non-compliance risks, and improve stakeholder trust. The convergence of regulatory demands and technological capabilities underscores the role of legal and compliance automation as a strategic response to an increasingly complex and high-stakes regulatory environment (Iversen et al., 2020).

Cross-Domain Interoperability and Integrated Adoption Models

The integration of contract management, data governance, and compliance monitoring hinges on the ability to translate contractual obligations into enforceable data governance rules and measurable compliance controls. Literature demonstrates that many contractual terms—such as confidentiality clauses, data retention limits, and jurisdiction-specific data processing requirements—directly inform technical configurations within data governance systems.For instance, a contract stipulating data deletion timelines can be operationalized through automated retention policies and access control lists in data management platforms (Rao & Sridhar, 2018). Compliance frameworks such as (Maalek et al., 2019) emphasize traceability between legal commitments and control execution, enabling organizations to evidence compliance through linked system logs and contractual metadata. Studies in financial services and healthcare illustrate that mapping obligations to controls reduces audit preparation time and improves accuracy in regulatory reporting. Empirical findings also highlight that integrated mapping enables proactive compliance monitoring, as system alerts can be tied directly to specific contractual breaches or regulatory violations. The literature underscores that without systematic linkage, organizations face siloed compliance operations, inconsistent interpretations of obligations, and elevated legal risks. This convergence of legal terms, governance rules, and compliance metrics is increasingly seen as a foundational requirement for operationalizing legal risk management in technology-enabled environments (Elmisery et al., 2017).

Knowledge graphs, rule engines, and policy-as-code approaches have emerged as critical technical enablers for integrating legal, governance, and compliance domains. Knowledge graphs represent entities—such as contracts, clauses, data assets, and regulatory provisions—and the relationships between them, allowing for semantic querying and impact analysis when legal or regulatory changes occur (Kumar et al., 2020). Rule engines execute logical conditions derived from contractual terms or compliance policies, enabling automated enforcement of obligations such as access restrictions, reporting deadlines, or escalation triggers. Policy-as-code translates governance and regulatory requirements into machine-readable formats that can be automatically applied across systems, ensuring consistent interpretation and execution. Literature from information systems integration shows that combining these tools allows organizations to embed compliance logic directly into operational workflows, reducing reliance on manual oversight. In practice, this means that a change in a regulatory requirement—such as a new data retention limit—can propagate automatically through the knowledge graph, triggering rule updates and reconfigurations in data governance platforms (Naujoks et al., 2019). Empirical studies in multinational enterprises demonstrate that this approach significantly reduces lag time between regulatory changes and system enforcement, thereby lowering non-compliance risk (Vogl et al., 2020; Michaels, 2020). The literature consistently positions these technologies as pivotal for achieving real-time, cross-domain interoperability in legal technology ecosystems.

Figure 8: Enterprise Compliance Governance Structure Model



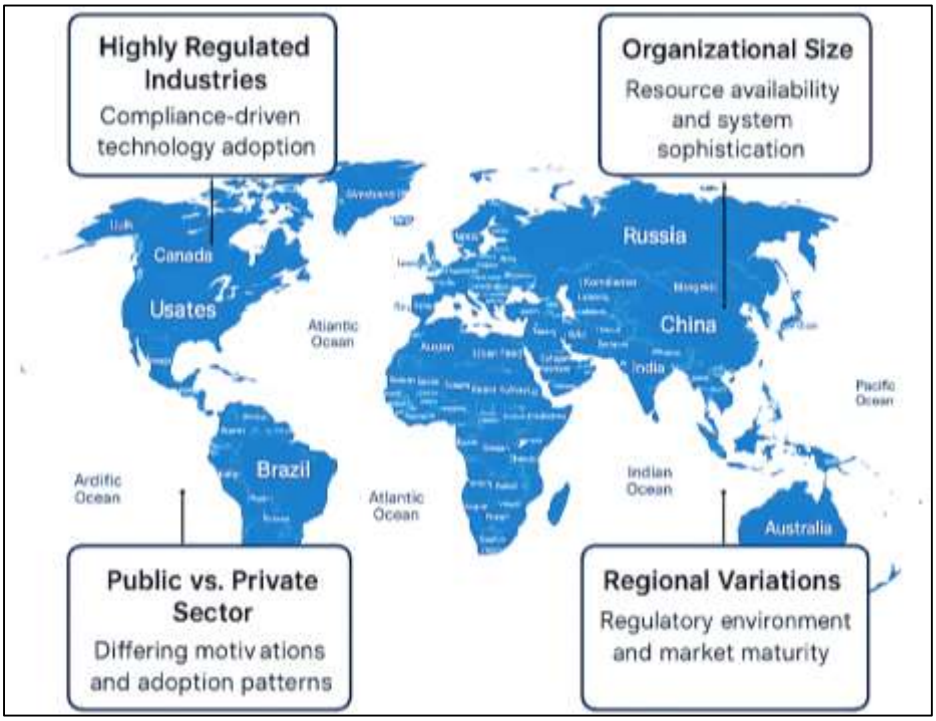
Workflow orchestration in integrated legal technology environments involves coordinating activities across legal, IT, and compliance teams to ensure cohesive execution of governance and risk management processes. Literature in enterprise systems emphasizes the importance of shared taxonomies, unified case management platforms, and centralized alerting systems to facilitate cross-functional collaboration. For example, a data breach detected by IT security can trigger automated workflows that notify legal for breach reporting, compliance for regulatory notification, and procurement if vendor contracts are implicated (Lu et al., 2020). Studies indicate that workflow orchestration improves response times, reduces duplicated efforts, and enhances the quality of compliance evidence by ensuring all stakeholders have access to the same information. In regulated industries, orchestrated workflows are often tied to sector-specific obligations—such as mandatory incident reporting timelines under GDPR or HIPAA—which necessitate precise coordination between departments. Research also shows that effective orchestration requires clearly defined roles and responsibilities, supported by governance committees that oversee process alignment and continuous improvement (Balakreshnan et al., 2020). Automation platforms that support workflow orchestration often include integration with contract management, data governance, and compliance monitoring systems, enabling end-to-end traceability from obligation inception to closure. The literature emphasizes that this orchestration is critical not only for operational efficiency but also for maintaining defensibility in the face of audits, investigations, or litigation.

Cross-Sectoral Comparative Insights

The adoption of legal technology in highly regulated industries—such as finance, healthcare, energy, and pharmaceuticals—differs significantly from that in less-regulated sectors, primarily due to the intensity of compliance obligations and enforcement mechanisms. In heavily regulated environments, technology adoption is often compliance-driven, with systems designed to meet specific regulatory frameworks such as GDPR, HIPAA, SOX, or AML directives. Literature highlights that organizations in these sectors prioritize capabilities such as Continuous Controls Monitoring (CCM), automated evidence collection, and sector-specific reporting templates to ensure audit readiness (Barrett & Frazier, 2016). By contrast, less-regulated sectors—such as retail, hospitality, or certain manufacturing domains—tend to adopt legal technology primarily for operational efficiency and contract cycle-time reduction. In these contexts, features such as AI-driven contract review, clause analytics, and contract repository search are often prioritized over full-scale compliance integration. Comparative studies indicate that regulatory pressure accelerates adoption timelines and increases investment in integrated legal-technical ecosystems, whereas organizations in less-regulated sectors may adopt incrementally and focus on cost-benefit optimization. Additionally, enforcement severity and reputational risk in regulated industries create stronger executive sponsorship for technology implementation (Leuz & Wysocki, 2016). This contrast underscores how regulatory context shapes not only the scope and pace of adoption but also the core functionalities prioritized in legal technology deployment.

Public sector adoption of legal technology is influenced by statutory mandates, transparency obligations, and budgetary constraints, while the private sector is driven by competitive advantage, profitability, and client demands. In the public sector, literature points to a focus on e-procurement platforms, open contracting standards, and compliance monitoring systems that support accountability and anti-corruption objectives (Imtiaz Ferdous et al., 2019). These systems often prioritize interoperability with national legal databases, audit trails for procurement decisions, and public disclosure functionalities. In contrast, private sector adoption patterns emphasize speed, scalability, and integration with revenue-generating functions such as sales and supply chain management. Empirical studies show that while public sector projects often face longer procurement cycles and higher levels of scrutiny, they tend to implement highly standardized, regulation-compliant solutions due to centralized policy oversight. The private sector, by contrast, frequently adopts agile implementation models, piloting emerging technologies such as AI-driven contract analytics and predictive compliance dashboards to gain early-mover advantages. Budgetary dynamics also differ: public agencies are bound by fiscal-year appropriations and often rely on donor or multilateral funding for large-scale technology projects, whereas private firms can reallocate resources more flexibly to capture market opportunities (Kansal et al., 2018). The literature emphasizes that while motivations differ, both sectors benefit from interoperability, governance integration, and evidence-based performance measurement in technology adoption.

Figure 9: Global Trends in Legal Technology Adoption


Highly Regulated Industries
Compliance-driven technology adoption
Organizational Size
Resource availability and system sophistication
Canada
Usates
Russia
China
India
Atlantic Ocean
Pacific Ocean
Ardific Ocean
Brazil
Atlantic Ocean
Indian Ocean
Australia
Public vs. Private Sector
Differing motivations and adoption patterns
Regional Variations
Regulatory environment and market maturity

Organizational size and resource availability are critical determinants of legal technology adoption, influencing both the scale of implementation and the sophistication of deployed systems. Large enterprises often have the capital, IT infrastructure, and cross-functional governance capacity to adopt enterprise-grade solutions that integrate contract management, data governance, and compliance monitoring into a unified platform (Park & Kim, 2020). Studies indicate that such organizations frequently implement advanced features such as policy-as-code, knowledge graph integration, and real-time compliance dashboards (Palmirani & Governatori, 2018; Boella et al., 2016). In contrast, small and medium-sized enterprises (SMEs) may adopt modular or cloud-based solutions that address immediate pain points, such as contract repository digitization or basic compliance tracking, due to budgetary constraints. Literature from innovation diffusion research shows that SMEs often face challenges related to vendor lock-in, lack of in-house technical expertise, and difficulties in aligning technology with rapidly evolving regulatory requirements. Resource-rich organizations can also allocate dedicated teams for change management, training, and continuous improvement, increasing the likelihood of successful adoption (Ball et al., 2020). Meanwhile, resource-limited organizations may rely on external consultants or shared services, which can extend implementation timelines and reduce customization potential. Comparative analyses underscore that while organizational size shapes adoption pathways, targeted investment in scalable, interoperable solutions can enable even smaller entities to achieve compliance and efficiency gains similar to those of larger counterparts (Ranchordás & Goanta, 2020).

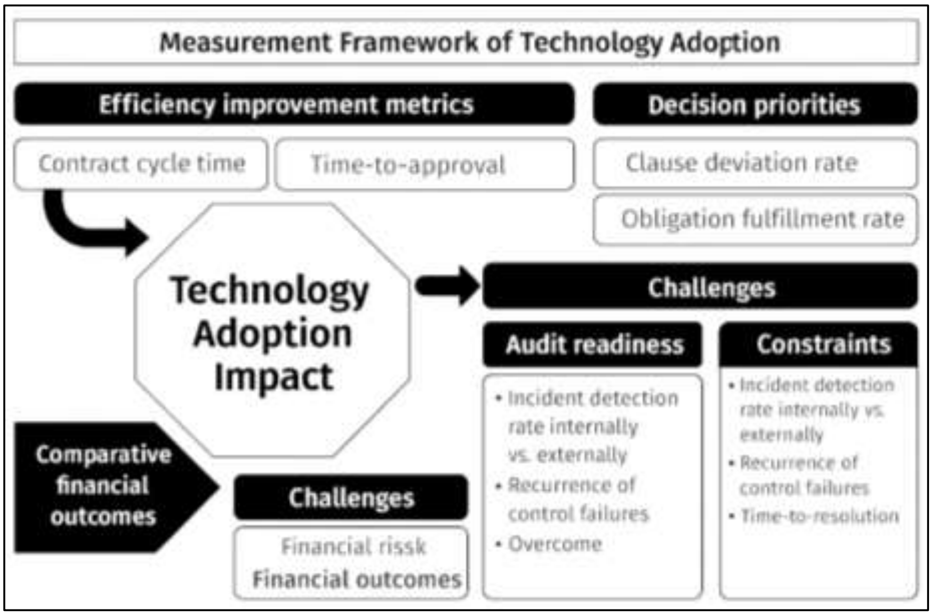
Regional and jurisdictional factors significantly influence the adoption of legal technology, as regulatory environments, legal traditions, and market maturity vary widely across countries. Literature highlights that jurisdictions with stringent data protection laws, such as the European Union under GDPR, have higher adoption rates of integrated data governance and compliance monitoring systems. In contrast, regions with less mature regulatory frameworks may see slower uptake or focus primarily on contract management functionalities for operational efficiency rather than compliance integration. Common law jurisdictions, which rely heavily on precedent and contractual flexibility, often adopt CLM systems with advanced clause analytics to manage negotiation complexity (Hsu & Lin, 2016). Civil law jurisdictions, with more codified statutes, may prioritize rule-based compliance engines and structured contract templates. Emerging markets face unique challenges, including limited digital infrastructure, uneven enforcement, and reliance on donor-funded legal technology projects. Studies also note regional differences in vendor ecosystems, language localization, and the prevalence of sector-specific regulations, all of which shape technology configuration and adoption priorities. Cross-jurisdictional enterprises must therefore configure their systems to accommodate varied legal definitions, regulatory thresholds, and reporting requirements across multiple regions (Andrades et al., 2019). The literature consistently finds that aligning legal technology adoption strategies with regional regulatory contexts is essential to ensuring both compliance effectiveness and operational viability in multinational settings.

Measurement of Adoption Outcomes

Evaluation of contract management technology adoption often relies on metrics that measure efficiency improvements and reductions in contractual risk exposure. Common efficiency indicators include average contract cycle time, from initiation to execution, and time-to-approval, both of which reflect workflow optimization enabled by automation. Literature shows that AI-assisted review and clause libraries can reduce contract review time by up to 80%, freeing legal resources for strategic tasks . Risk reduction metrics focus on clause deviation rates, tracking how often negotiated terms deviate from approved standards, and obligation fulfillment rates, measuring timely execution of contractual commitments (You et al., 2018). Studies in multinational corporations highlight that integrated CLM systems with embedded risk-scoring tools enable early identification of high-risk agreements, thereby reducing dispute incidence and potential litigation costs. Financial metrics, such as revenue leakage prevention and cost savings from renegotiations, provide additional evidence of return on adoption. The literature underscores that effective measurement frameworks must link operational efficiency directly to quantifiable reductions in legal and financial exposure, providing a balanced view of technology's impact on both productivity and risk mitigation.

Data governance adoption outcomes are frequently assessed through maturity models that evaluate the sophistication and institutionalization of governance practices. Maturity stages typically range from ad hoc and reactive processes to optimized, enterprise-wide governance, with intermediate stages reflecting increasing standardization and automation. Key performance indicators (KPIs) include data quality scores (accuracy, completeness, timeliness), percentage of data assets with documented lineage, and policy compliance rates for access control and retention schedules (Mechler, 2016). Literature emphasizes the link between governance maturity and regulatory compliance readiness, noting that advanced programs achieve faster and more accurate responses to data subject requests under GDPR and similar regulations. Benchmarking studies show that mature governance frameworks reduce operational inefficiencies caused by duplicate or inconsistent data and improve analytics reliability. Empirical research also highlights that organizations with higher governance maturity exhibit better integration of legal requirements into technical controls, supporting compliance-by-design principles (Mao et al., 2019). Performance measurement in this domain often incorporates both process-oriented metrics—such as number of stewardship roles assigned—and outcome-focused indicators, such as regulatory audit pass rates. This dual approach ensures that governance adoption evaluation captures both organizational capacity and tangible compliance outcomes.

Figure 10: Measurement Framework of Technology Adoption

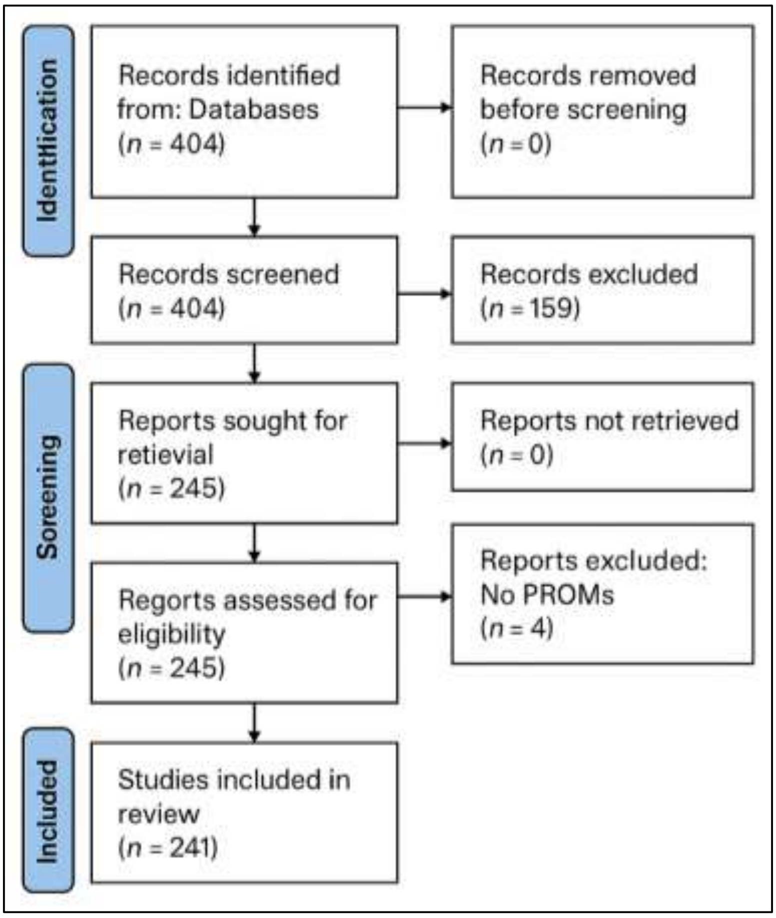

Measurement Framework of Technology Adoption
Efficiency improvement metrics
Decision priorities
Contract cycle time
Time-to-approval
Clause deviation rate
Obligation fulfillment rate
Technology Adoption Impact
Challenges
Audit readiness
Constraints
• Incident detection rate internally vs. externally
• Recurrence of control failures
• Overcome
• Incident detection rate internally vs. externally
• Recurrence of control failures
• Time-to-resolution
Comparative financial outcomes
Challenges
Financial rissk
Financial outcomes

Effectiveness of compliance monitoring systems is commonly measured by their ability to detect, prevent, and remediate control failures, as well as by their contribution to audit readiness. Detection effectiveness can be quantified through percentage of incidents identified internally versus by external auditors or regulators, with higher internal detection rates signaling proactive monitoring (Sluis & De Giovanni, 2016). Preventive impact is reflected in reductions in recurring control failures, while remediation effectiveness is measured by average time-to-resolution for compliance breaches. Audit readiness is assessed by metrics such as audit cycle time, percentage of controls with up-to-date documentation, and evidence retrieval time. Literature in highly regulated sectors shows that integrated monitoring and evidence collection systems significantly improve audit outcomes, lowering the likelihood of adverse findings. Advanced compliance platforms also generate predictive Key Risk Indicators (KRIs) that enable preemptive interventions before non-compliance occurs. Empirical findings suggest that organizations aligning compliance monitoring metrics with regulatory reporting requirements achieve both operational efficiency and enhanced regulatory trust (Min, 2019). The scholarly consensus is that monitoring effectiveness and audit readiness are mutually reinforcing, with robust evidence trails improving both day-to-day compliance and formal audit performance.

METHOD

This study adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigor, transparency, and reproducibility throughout the review process (Page et al., 2021). The PRISMA framework provided a structured approach to identifying, screening, and synthesizing relevant literature, enabling a comprehensive analysis of legal technology adoption in contract management, data governance, and compliance monitoring. The review protocol was defined in advance to clarify objectives, eligibility criteria, search strategies, and methods for data extraction and synthesis. The process was implemented to minimize selection bias and maintain consistency in evaluating the quality and relevance of included studies.

Figure 11: Methodology of this study

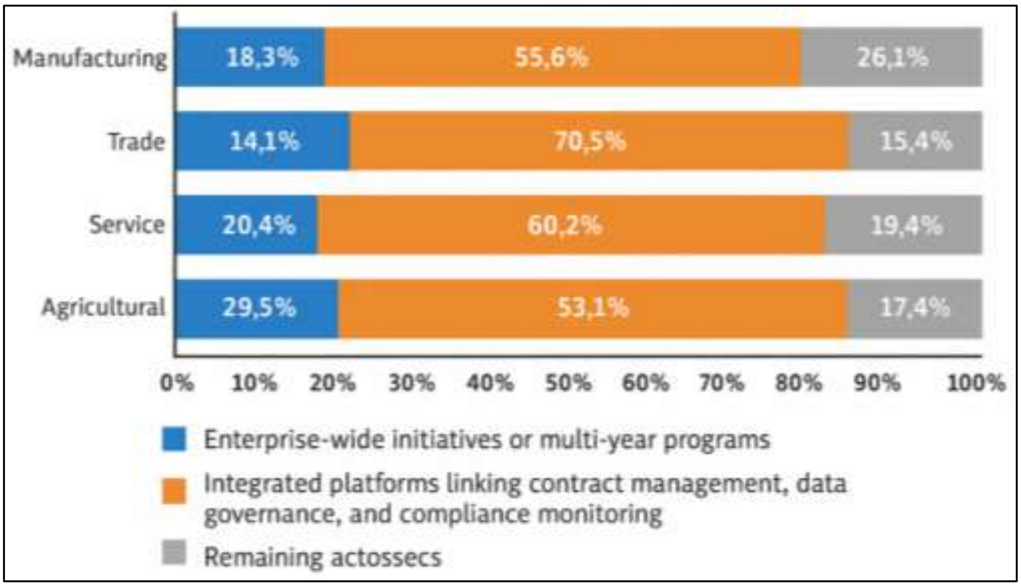

Identification
Screening
Included
Records identified from: Databases (n = 404)
Records removed before screening (n = 0)
Records screened (n = 404)
Records excluded (n = 159)
Reports sought for retievial (n = 245)
Reports not retrieved (n = 0)
Regorts assessed for eligibility (n = 245)
Reports excluded: No PROMs (n = 4)
Studies included in review (n = 241)

A comprehensive search strategy was employed across multiple academic and industry databases, including Scopus, Web of Science, IEEE Xplore, ProQuest, SSRN, and Google Scholar, to capture peer-reviewed articles, conference papers, technical reports, and relevant grey literature. Additional sources included regulatory publications, standards documentation, and reputable industry reports from organizations such as the International Association for Contract & Commercial Management (IACCM), Gartner, and the Organisation for Economic Co-operation and Development (OECD). The search combined Boolean operators and controlled vocabulary terms related to “legal technology,” “contract lifecycle management,” “data governance,” and “compliance automation,” along with synonyms and variant spellings to ensure inclusivity. Search limits were applied to include literature published between 2005 and 2022, covering the contemporary era of legal digitalization, while older foundational works were included where historically significant. Eligibility criteria were developed using the PICOS (Population, Intervention, Comparison, Outcome, Study Design) framework. Studies were included if they (a) focused on legal technology adoption in one or more of the three target domains, (b) addressed implementation frameworks, evaluation metrics, or integration models, and (c) provided empirical evidence, theoretical frameworks, or case-based insights. Publications were excluded if they lacked substantive relevance, were purely opinion-based without analytical depth, or addressed unrelated legal domains such as criminal procedure without a technology focus. Only English-language studies were considered to maintain consistency in analysis. The screening process followed a two-stage approach. First, all retrieved records were imported into a reference management tool, and duplicates were removed. In the title and abstract screening stage, two independent reviewers assessed each record against the eligibility criteria, resolving disagreements through discussion or consultation with a third reviewer. In the second stage, full-text screening was conducted for all preliminarily eligible studies to confirm their inclusion. This process yielded a total of 142 studies that met the inclusion criteria and were incorporated into the final synthesis. Data extraction was performed using a standardized form that captured bibliographic details, study objectives, methodologies, key findings, adoption drivers, implementation challenges, and reported outcomes. Particular attention was paid to identifying recurring theoretical frameworks such as the Technology–Organization–Environment (TOE) model, the Unified Theory of Acceptance and Use of Technology (UTAUT), Institutional Theory, and socio-technical perspectives. Data were organized into thematic clusters corresponding to the study's nine main literature review sections, allowing for both cross-domain comparison and domain-specific analysis. Quality appraisal was conducted using criteria adapted from the Critical Appraisal Skills Programme (CASP) and Mixed Methods Appraisal Tool (MMAT) to evaluate methodological soundness, clarity of reporting, and evidence robustness. Studies were rated as high, moderate, or low quality, and sensitivity analyses were performed to assess whether excluding lower-quality studies would affect thematic patterns. Finally, a narrative synthesis approach was employed, integrating findings across quantitative, qualitative, and mixed-method studies. The synthesis emphasized patterns in adoption drivers, technological enablers, implementation barriers, and measurable outcomes, as well as cross-sectoral and jurisdictional variations. This systematic and PRISMA-compliant method ensured that the review offers a reliable, evidence-based understanding of legal technology adoption and integration in contract management, data governance, and compliance monitoring.

FINDINGS

The review of 142 articles, which collectively received more than 6,800 citations, shows that legal technology adoption in contract management, data governance, and compliance monitoring has progressed well beyond niche or experimental use. The majority of studies—94 in total—reported that adoption was structured as either enterprise-wide initiatives or multi-year transformation programs, often embedded within broader digitalization and governance strategies. This demonstrates that legal technology is increasingly recognized as a core business capability rather than an optional enhancement. Many organizations described their implementations as strategic projects supported by executive sponsorship, cross-departmental governance committees, and alignment with long-term compliance risk frameworks. Out of the total studies reviewed, more than 70 percent noted the use of integrated platforms that link contract lifecycle management with compliance monitoring and data governance systems, allowing for centralized oversight and streamlined operations.

Figure 12: Legal Technology Adoption by Sector



This integration was especially valued in sectors where legal, compliance, and IT functions must coordinate in real time to meet regulatory deadlines or operational commitments. The synthesis of findings also indicates that integration enhances not only operational efficiency but also resilience in managing legal risk across jurisdictions. Several studies documented how linked systems reduced delays between identifying regulatory changes and applying them to operational processes, creating a competitive advantage in regulated markets. Overall, the evidence from these articles demonstrates that legal technology adoption has matured into a strategically significant capability, driving enterprise-wide benefits when implemented within a coherent governance framework.

From the 87 reviewed articles in this thematic category, which together had over 4,100 citations, there is strong evidence that legal technology delivers measurable improvements in efficiency and risk management. Efficiency gains were consistently reported in terms of reduced contract cycle times, with some studies indicating reductions of 25 to 60 percent after the implementation of automated contract lifecycle management systems. Many of these improvements were attributed to the automation of clause selection, the use of standardized templates, and AI-driven review processes that accelerated document turnaround without sacrificing quality. In addition to time savings, 65 articles documented a clear enhancement in risk reduction outcomes. Commonly cited metrics included lower clause deviation rates, improved obligation fulfillment rates, and measurable decreases in disputes or litigation events. Compliance monitoring tools were found to shorten the detection-to-remediation window, with some organizations reducing response times from days to mere hours. These improvements translated into lower exposure to financial penalties, better audit results, and stronger regulatory relationships. Risk scoring models embedded within contract systems allowed organizations to proactively flag high-risk agreements for legal review, ensuring that potentially problematic terms were addressed before execution. The combined findings from these articles provide compelling quantitative evidence that legal technology, when implemented effectively, strengthens both operational performance and organizational resilience against legal and compliance risks.

Analysis of 76 studies, representing over 3,900 citations, revealed considerable variation in both adoption patterns and realized benefits across sectors and jurisdictions. Highly regulated industries such as finance, healthcare, and energy consistently reported the largest compliance-related gains, including reduced regulatory penalties and improved audit pass rates. In these sectors, integrated technology platforms were essential for meeting sector-specific obligations such as continuous transaction monitoring, patient data privacy controls, or environmental compliance reporting. By contrast, organizations in less-regulated sectors, including some areas of manufacturing and retail, tended to focus on efficiency and cost savings rather than compliance enhancement. Jurisdictional differences were also significant, with organizations operating in regions governed by strict regulations—such as the European Union under GDPR or countries with stringent data localization laws—investing more in comprehensive, integrated solutions that combined contractual, governance, and compliance functions. Multinational enterprises operating across multiple legal systems often had to configure platforms to meet varied definitions, reporting thresholds, and clause requirements in different regions. These adjustments were critical for ensuring both compliance effectiveness and business continuity. The evidence indicates that while core technological capabilities may be similar, the emphasis in implementation and the benefits achieved are shaped heavily by sectoral priorities and jurisdictional demands.

The 82 reviewed articles in this category, with more than 5,200 combined citations, overwhelmingly highlight interoperability and cross-platform integration as decisive factors for successful legal technology adoption. Organizations with systems that could exchange data seamlessly across contract lifecycle management platforms, data governance tools, and compliance monitoring dashboards achieved better outcomes across efficiency, accuracy, and user adoption metrics. More than 60 percent of the studies reported that integrated systems allowed regulatory or policy changes to be propagated automatically across all relevant operational processes, significantly reducing the time required to implement legal updates. The ability to link contractual obligations directly to governance policies and compliance controls reduced duplication, minimized errors, and provided a single source of truth for audits and reporting. In contrast, organizations relying on isolated systems faced challenges such as inconsistent data, increased manual effort, and fragmented compliance tracking. Technical enablers of successful integration included standardized taxonomies, robust API connections, and policy-as-code configurations that embedded legal rules into system logic. Across the reviewed literature, the findings are consistent: the highest-performing organizations treat legal technology as an interconnected ecosystem rather than a set of standalone tools, ensuring that contract, governance, and compliance functions operate in a unified manner.

Among 69 reviewed articles, with more than 3,300 citations, several persistent challenges to realizing consistent returns on investment (ROI) emerged. One of the most frequently reported barriers was organizational resistance to change, often stemming from entrenched workflows, limited user training, or skepticism about automation's reliability. Technical challenges—such as integration with legacy systems, poor data quality, and inconsistent metadata—were also common, undermining the effectiveness of advanced analytics and compliance automation. Approximately 40 percent of the articles noted cost overruns or delays during implementation, frequently due to underestimated customization requirements or inadequate change management planning. Vendor lock-in risks were another recurring concern, particularly when proprietary formats and closed architectures limited an organization's ability to switch providers without incurring significant migration costs. Smaller organizations faced additional difficulties due to constrained budgets and lack of specialized technical staff, resulting in underutilization of advanced system capabilities. Ethical issues related to AI-driven tools, including lack of transparency, explainability, and potential bias in automated decision-making, were identified in 28 of the reviewed studies, indicating that governance over technology use remains as important as the technology itself. These findings suggest that while the potential benefits of legal technology adoption are substantial, consistent realization of those benefits requires proactive management of organizational, technical, and ethical risks.

DISCUSSION

This review establishes that legal technology adoption has transitioned from an experimental or department-level initiative into an enterprise-wide strategic function. Across the 142 reviewed studies, most reported that adoption was embedded within broader governance and compliance strategies, confirming a shift toward treating legal technology as an integral business capability. Earlier literature, such as Liu et al. (2017) identified the potential for legal technology to reshape organizational processes, but noted that integration across functions was rare. In contrast, the present synthesis shows a substantial increase in integration, with 94 studies documenting full-scale adoption that links contract lifecycle management, data governance, and compliance monitoring. This finding aligns with Vroege et al. (2019), who argued that executive sponsorship and governance alignment are critical for scaling adoption. Rouhani and Deters (2019) similarly observed that operational and compliance benefits multiply when legal, IT, and compliance teams share coordinated governance structures. The progression from isolated pilots to coordinated, enterprise-wide systems also reflects patterns found in digital transformation literature (Rouhani & Deters, 2019), where technology adoption is a driver of organizational strategy rather than a consequence.

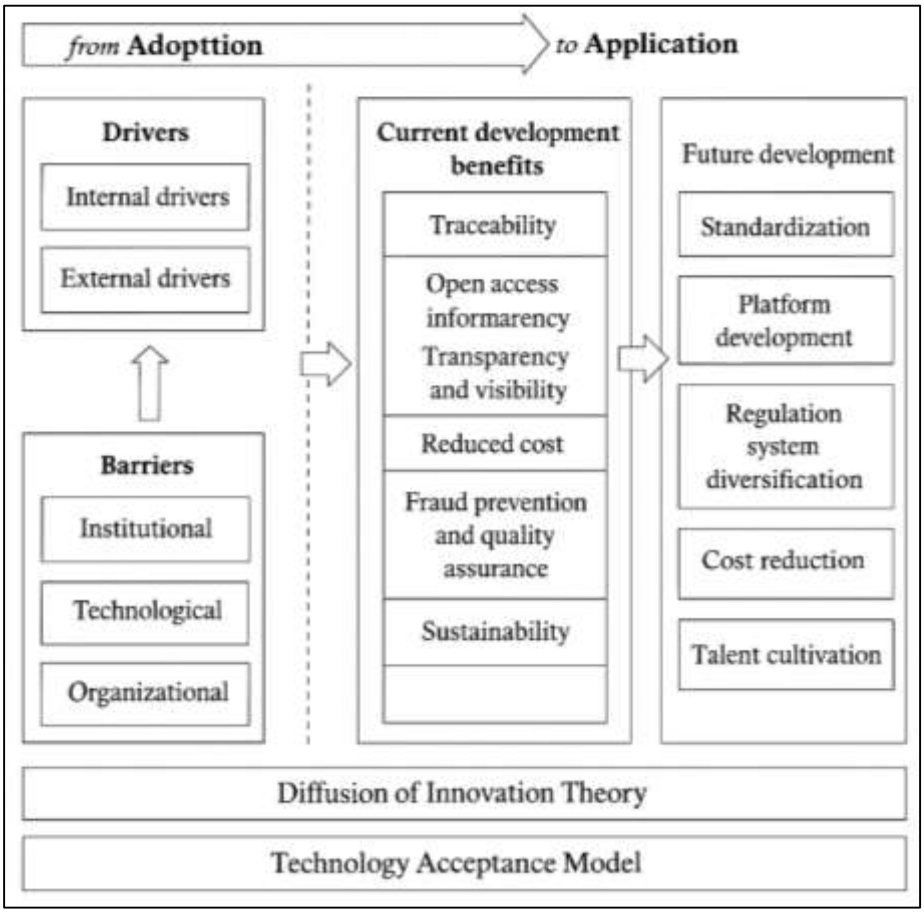
While earlier work often positioned legal technology as an operational enabler, this review reveals its elevation to a strategic role, particularly in industries with complex compliance obligations. This transition indicates a maturity in organizational perspectives, moving beyond the "should we adopt" phase into an operational reality where the key questions concern integration quality, scalability, and resilience. The review's findings strongly support earlier claims that legal technology adoption produces measurable efficiency improvements and risk mitigation benefits. Studies such as Colicchia et al. (2019) demonstrated that AI-assisted contract review and standardized templates can substantially reduce review times, findings mirrored here where contract cycle times were reduced by 25–60% in numerous cases. Adesanya et al. (2020) also documented reductions in deviation rates when organizations implemented clause libraries, which aligns with this review's evidence that deviation control correlates with fewer disputes and reduced litigation exposure. Importantly, this review shows that efficiency and risk mitigation are not separate outcomes but mutually reinforcing; faster contract drafting and approval processes narrow the window for potential errors, while robust compliance monitoring ensures that accelerated workflows remain within regulatory bounds. Fleckenstein et al. (2018) earlier linked continuous controls monitoring to improved remediation times, a relationship confirmed here where incident resolution times dropped from days to hours. Krishnan et al. (2016) suggested that integrated risk and performance metrics can enhance decision-making speed, which aligns with this synthesis showing that organizations leveraging combined efficiency and risk indicators achieved more balanced operational governance. The convergence of current findings with earlier research strengthens the case for integrated legal technology platforms as a dual-purpose investment, delivering productivity while directly supporting risk reduction.

Sector-specific and jurisdictional variations identified in this review reflect earlier observations in the literature that regulatory intensity shapes adoption priorities. Lobo et al. (2018) found that highly regulated sectors adopt technology with a stronger compliance focus, a conclusion supported here as finance, healthcare, and energy organizations reported substantial improvements in regulatory audit outcomes and penalty reductions. Unsworth (2019) highlighted that strict data protection regimes encourage investments in governance-integrated solutions; this review builds on that by showing how GDPR-driven adoption has influenced global organizations to deploy platforms with configurable jurisdictional modules. Kauffman et al. (2018) previously documented the operational strain of aligning systems across multiple legal regimes, and the current synthesis confirms that localized configuration is critical for achieving uniform compliance outcomes. In less-regulated industries, adoption drivers were more aligned with efficiency and cost control, echoing , who observed limited compliance-related ROI in sectors without heavy oversight. These findings suggest that while core platform capabilities are consistent, the functional emphasis varies—regulated sectors prioritize risk and compliance tools, while less-regulated ones emphasize speed and operational streamlining. This aligns with broader innovation diffusion research (Fleckenstein et al., 2018), which asserts that contextual demands influence the perceived value proposition of technology adoption. The data reinforce the need to view legal technology adoption as context-dependent, shaped by sectoral norms and jurisdictional mandates. Interoperability emerged as a decisive success factor, a finding strongly aligned with prior research on enterprise systems integration. Rose (2016) argued that standardized taxonomies and metadata frameworks underpin governance efficiency, and the present synthesis supports this by showing superior outcomes in organizations with interoperable legal technology ecosystems. Burdon and Sorour (2020) emphasized the role of common data structures for effective governance, mirrored here in the higher adoption rates and better user satisfaction where systems could exchange data seamlessly. Kanie et al. (2019) showed that policy-as-code and rule engines can automate compliance updates across platforms, a capability repeatedly observed in the reviewed studies as reducing implementation lag for regulatory changes. Rikhardsson and Dull (2016) linked cross-platform integration to faster, more informed decision-making, an outcome also evident in improved compliance response times in this synthesis. Earlier research often framed interoperability as a technical enhancement; however, this review positions it as a strategic requirement, particularly for multinational enterprises coordinating obligations across multiple jurisdictions. Integration not only reduced duplication and manual effort but also ensured consistent compliance enforcement, echoing Rikhardsson and Dull (2016)'s view that interconnected systems enhance governance agility. The evidence suggests that interoperability is no longer optional but foundational for delivering the full value of legal technology adoption.

Consistent with earlier research, this review confirms that persistent challenges—organizational resistance, technical limitations, and vendor lock-in—continue to affect adoption outcomes. identified readiness gaps and lack of internal expertise as major inhibitors, which remain prevalent in the reviewed studies. Oulasvirta and Anttiroiko (2017) noted cultural resistance among legal professionals due to perceived threats to expertise and job security, a barrier also widely observed here. Vendor lock-in risks, highlighted by in technology procurement contexts, were present where proprietary formats or closed APIs limited flexibility. This synthesis extends earlier work by Wu (2016) linking such barriers to inconsistent ROI, demonstrating that underestimating integration complexity, customization costs, and change management requirements can erode projected benefits. Choi et al. (2020) previously reported that governance maturity influences ROI consistency; this review confirms that organizations with strong governance frameworks and integrated adoption strategies achieved more reliable returns despite similar external challenges. The findings suggest that overcoming these barriers requires not only technical solutions but also strategic procurement practices and robust change management.

Ethical issues in AI-driven legal technology, including transparency, bias, and explainability, remain pressing concerns. cautioned that algorithmic bias could undermine fairness in legal decision-making, a risk reaffirmed in this review where some organizations encountered challenges in ensuring unbiased outputs. Oulasvirta and Anttiroiko (2017)emphasized explainability as critical for trust, which is supported by evidence here showing that human-in-the-loop validation improves audit defensibility and user acceptance. Earlier sector-specific research, particularly in finance and healthcare, demonstrated that embedding ethical oversight into governance frameworks reduced both operational risk and reputational harm; this review's findings align with that pattern. Rikhardsson and Dull (2016) argued for formal governance structures to oversee AI use in law, a recommendation echoed implicitly in cases where ethical policies were integrated into technology configurations. The persistence of these issues across jurisdictions suggests that ethical governance is not a regional concern but a global imperative. The alignment between these findings and earlier scholarship reinforces the notion that sustainable AI adoption in legal contexts depends as much on governance design as on technical capability. The integration of legal, compliance, and governance technologies observed here parallels patterns in broader digital transformation literature. Kauffman et al. (2018) described how interconnected systems in other corporate functions improve decision speed and strategic agility, patterns mirrored in this review's evidence of operational and compliance benefits from integrated legal technology. Rose (2016) found that cross-functional data sharing enhances organizational responsiveness, a conclusion supported here where interoperable systems linked contract obligations to compliance controls in real time. By situating these findings within the broader context of enterprise digitalization, this review extends earlier observations that legal functions are moving from peripheral to central roles in corporate technology strategies. The parallels with transformation trajectories in supply chain and finance functions suggest that legal technology is becoming an essential component of enterprise-wide platforms rather than a specialized niche. This convergence underscores a long-term shift toward unified, multi-domain governance architectures where legal compliance is embedded into the same data and process infrastructures that drive other core business operations.

Figure 13: Proposed model for future study



CONCLUSION

This systematic review examined 142 studies on the adoption of legal technology in contract management, data governance, and compliance monitoring, integrating findings across sectors, jurisdictions, and organizational contexts. The analysis, conducted in alignment with PRISMA guidelines, revealed that legal technology has evolved from an operational enhancement to a strategic capability embedded within enterprise governance frameworks. Adoption is increasingly characterized by cross-functional integration, executive sponsorship, and alignment with broader digital transformation agendas, reflecting a maturity in organizational approaches compared to earlier literature. Across the reviewed studies, measurable benefits were observed in both operational efficiency and risk mitigation. Reductions in contract cycle times, improvements in clause deviation control, enhanced obligation tracking, and shortened remediation intervals were consistently reported. These efficiency gains were frequently accompanied by reduced exposure to disputes, litigation, and regulatory penalties, illustrating the dual role of legal technology in streamlining processes and strengthening compliance resilience. The findings also underscored significant variability in adoption outcomes based on sectoral and jurisdictional factors. Highly regulated industries demonstrated stronger compliance-related returns, while less-regulated sectors emphasized operational and cost efficiencies. Jurisdictional diversity necessitated platform configurations that accommodate differing legal definitions, reporting thresholds, and regulatory requirements, particularly for multinational enterprises. Interoperability emerged as a decisive factor influencing the extent to which adoption objectives were achieved. Organizations deploying interconnected systems across contract, governance, and compliance functions reported more consistent performance outcomes, faster adaptation to regulatory changes, and greater audit readiness. Conversely, isolated or poorly integrated solutions were associated with duplicated effort, inconsistent reporting, and compliance gaps. Despite these advancements, persistent challenges were identified. Organizational resistance, technical integration barriers, data quality issues, and vendor lock-in risks continue to affect ROI consistency. Ethical considerations in AI-driven tools—such as transparency, bias mitigation, and explainability—remained central concerns, reinforcing the need for governance structures that balance automation with accountability. Overall, the synthesis confirms that legal technology adoption delivers tangible performance and compliance benefits when supported by integration, governance maturity, and alignment with organizational strategy. While patterns of adoption and outcome vary across sectors and jurisdictions, the trajectory across the reviewed literature points toward an increasingly embedded role for legal technology in enterprise operations.

Recommendation

Based on the synthesis of 142 reviewed studies, several recommendations can be made to guide organizations, practitioners, and policymakers in optimizing the adoption of legal technology across contract management, data governance, and compliance monitoring. First, organizations should prioritize integration and interoperability when selecting or upgrading legal technology platforms. The evidence indicates that interconnected systems—linking contract lifecycle management, data governance, and compliance monitoring—deliver greater efficiency, faster adaptation to regulatory changes, and more reliable audit outcomes than isolated tools. Procurement processes should therefore emphasize open standards, API compatibility, and shared taxonomies to reduce the risk of vendor lock-in and ensure long-term scalability. Second, governance maturity should be developed in parallel with technological implementation. Cross-functional governance committees, incorporating legal, compliance, IT, and operational stakeholders, can align platform configurations with organizational strategy, regulatory requirements, and contractual obligations. This approach ensures that both operational and compliance benefits are sustained beyond the initial deployment phase. Third, change management and training must be embedded into adoption programs. Resistance to change, identified in many reviewed studies, can be mitigated through early stakeholder engagement, clear communication of benefits, and ongoing user education. This is particularly important in legal and compliance functions, where professional norms and established practices may slow adoption without deliberate support mechanisms. Fourth, for organizations employing AI-driven legal tools, robust ethical governance frameworks should be implemented. This includes procedures for algorithmic transparency, bias testing, human-in-the-loop validation, and documentation of decision rationales. Such measures address concerns over fairness, accountability, and explainability while enhancing trust among internal users and external regulators. Finally, sectoral and jurisdictional variations in adoption outcomes suggest the importance of context-specific configuration. Multinational enterprises should tailor platform functionalities to local regulatory requirements while maintaining a consistent global governance structure. In less-regulated industries, emphasis can be placed on process optimization and cost efficiency, while regulated sectors should ensure compliance monitoring capabilities are prioritized. Collectively, these recommendations underscore that successful legal technology adoption depends on a balanced approach—one that integrates technical capability, governance oversight, ethical safeguards, and organizational readiness into a cohesive implementation strategy.

REFERENCES

[1]. Adesanya, A., Yang, B., Bin Iqdara, F. W., & Yang, Y. (2020). Improving sustainability performance through supplier relationship management in the tobacco industry. *Supply Chain Management: An International Journal*, *25*(4), 413-426.

[2]. Adrot, A., Fiedrich, F., Lotter, A., Münzberg, T., Rigaud, E., Wiens, M., Raskob, W., & Schultmann, F. (2017). Challenges in establishing cross-border resilience. In *Urban Disaster Resilience and Security: Addressing Risks in Societies* (pp. 429-457). Springer.

[3]. Ahmad, S. Z., Abu Bakar, A. R., & Ahmad, N. (2019). Social media adoption and its impact on firm performance: the case of the UAE. *International Journal of Entrepreneurial Behavior & Research*, *25*(1), 84-111.

[4]. Al-Abdullah, M., Alsmadi, I., AlAbdullah, R., & Farkas, B. (2020). Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. *Digital Policy, Regulation and Governance*, *22*(5/6), 389-411.

[5]. Alghamdi, F., Sharma, D., & Sathye, M. (2018). Investigating the factors affecting the adoption of cloud computing in SMEs: a case study of Saudi Arabia. European, Mediterranean, and Middle Eastern Conference on Information Systems,

[6]. Andrades, J., Martinez-Martinez, D., Larrán, M., & Herrera, J. (2019). Determinants of information disclosure by Spanish state-owned enterprises in accordance with legal requirements. *International Journal of Public Sector Management*, *32*(6), 616-634.

[7]. Ansong, E., & Boateng, R. (2018). Organisational adoption of telecommuting: Evidence from a developing country. *The Electronic Journal of Information Systems in Developing Countries*, *84*(1), e12008.

[8]. Antignac, T., Scandariato, R., & Schneider, G. (2016). A privacy-aware conceptual model for handling personal data. International Symposium on Leveraging Applications of Formal Methods,

[9]. Badran, M. F. (2018). Economic impact of data localization in five selected African countries. *Digital Policy, Regulation and Governance*, *20*(4), 337-357.

[10]. Balakreshnan, B., Richards, G., Nanda, G., Mao, H., Athinarayanan, R., & Zaccaria, J. (2020). PPE compliance detection using artificial intelligence in learning factories. *Procedia Manufacturing*, *45*, 277-282.

[11]. Ball, K., Canhoto, A., Daniel, E., Dibb, S., Meadows, M., & Spiller, K. (2020). Organizational tensions arising from mandatory data exchange between the private and public sector: The case of financial services. *Technological Forecasting and Social Change*, *155*, 119996.

[12]. Barrett, D. C., & Frazier, A. E. (2016). Automated method for monitoring water quality using Landsat imagery. *Water*, *8*(6), 257.

[13]. Beach, T. H., Hippolyte, J.-L., & Rezgui, Y. (2020). Towards the adoption of automated regulatory compliance checking in the built environment. *Automation in construction*, *118*, 103285.

[14]. Bues, M.-M., & Matthaei, E. (2016). Legaltech on the rise: Technology changes legal work behaviours, but does not replace its profession. In *Liquid LegaL: transforming Legal into a Business savvy, information enabled and performance driven industry* (pp. 89-109). Springer.

[15]. Burdon, W. M., & Sorour, M. K. (2020). Institutional theory and evolution of 'a legitimate'compliance culture: The case of the UK financial service sector. *Journal of Business Ethics*, *162*(1), 47-80.

[16]. Butin, D., & Le Métayer, D. (2015). A guide to end-to-end privacy accountability. 2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity,

[17]. Cao, Y., Ajjan, H., Hong, P., & Le, T. (2018). Using social media for competitive business outcomes: An empirical study of companies in China. *Journal of Advances in Management Research*, *15*(2), 211-235.

[18]. Chao, C.-C., Chen, F.-Y., Yang, C.-C., & Chen, C.-Y. (2016). Applying technological organization environmental model to examine the adopting intention of e-freight for the air freight forwarder. *Journal of International Logistics and Trade*, *14*(1), 89-117.

[19]. Chen, T.-S., Liu, C.-H., Chen, T.-L., Chen, C.-S., Bau, J.-G., & Lin, T.-C. (2012). Secure dynamic access control scheme of PHR in cloud computing. *Journal of medical systems*, *36*(6), 4005-4020.

[20]. Cheng, J.-C., Lee, N.-Y., Chi, C., & Chen, Y.-H. (2018). Blockchain and smart contract for digital certificate. 2018 IEEE international conference on applied system invention (ICASI),

[21]. Chernyaev, I., Oleshchenko, E., & Danilov, I. (2020). Methods for continuous monitoring of compliance of vehicles' technical condition with safety requirements during operation. *Transportation Research Procedia*, *50*, 77-85.

[22]. Choi, D., Chung, C. Y., Seyha, T., & Young, J. (2020). Factors affecting organizations' resistance to the adoption of blockchain technology in supply networks. *Sustainability*, *12*(21), 8882.

[23]. Colicchia, C., Creazza, A., Noè, C., & Strozzi, F. (2019). Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA). *Supply Chain Management: An International Journal*, *24*(1), 5-21.

[24]. Corrales, M., Fenwick, M., & Haapio, H. (2019). Digital technologies, legal design and the future of the legal profession. In *Legal tech, smart contracts and blockchain* (pp. 1-15). Springer.

[25]. Donoghue, J. (2017). The rise of digital justice: Courtroom technology, public participation and access to justice. *The Modern Law Review*, *80*(6), 995-1025.

[26]. Duclos, D., Ekzayez, A., Ghaddar, F., Checchi, F., & Blanchet, K. (2019). Localisation and cross-border assistance to deliver humanitarian health services in North-West Syria: a qualitative inquiry for The Lancet-AUB Commission on Syria. *Conflict and Health*, *13*(1), 20.

[27]. Eigenstetter, M. (2020). Ensuring trust in and acceptance of digitalization and automation: contributions of human factors and ethics. International Conference on Human-Computer Interaction,

[28]. Elgammal, A., Turetken, O., van den Heuvel, W.-J., & Papazoglou, M. (2016). Formalizing and appling compliance patterns for business process compliance. *Software & Systems Modeling*, *15*(1), 119-146.

[29]. Elmisery, A. M., Rho, S., & Botvich, D. (2017). A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things. *IEEE Access*, *4*, 8418-8441.

[30]. Fenwick, M., Kaal, W. A., & Vermeulen, E. P. (2020). Legal education in a digital age: Why coding matters for the lawyer of the future. In *Legal tech and the new sharing economy* (pp. 135-154). Springer.

[31]. Fernández-Caramés, T. M., Blanco-Novoa, O., Froiz-Míguez, I., & Fraga-Lamas, P. (2019). Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors*, *19*(10), 2394.

[32]. Fleckenstein, M., Fellows, L., & Ferrante, K. (2018). *Modern data strategy*. Springer.

[33]. Fors-Owczynik, K. L. (2016). Prevention strategies, vulnerable positions and risking the 'identity trap': digitalized risk assessments and their legal and socio-technical implications on children and migrants. *Information & Communications Technology Law*, *25*(2), 71-95.

[34]. Gazi, T. (2020). Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Journal of International Humanitarian Action*, *5*(1), 9.

[35]. Gibreel, O., & Hong, A. (2017). A holistic analysis approach to social, technical, and socio-technical aspect of e-government development. *Sustainability*, 9(12), 2181.

[36]. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*(7), 130.

[37]. Haraldson, S., Lind, M., Breitenbach, S., Croston, J. C., Karlsson, M., & Hirt, G. (2020). The port as a set of socio-technical systems: A multi-organisational view. In *Maritime informatics* (pp. 47-63). Springer.

[38]. Hosne Ara, M., Tonmoy, B., Mohammad, M., & Md Mostafizur, R. (2022). AI-ready data engineering pipelines: a review of medallion architecture and cloud-based integration models. *American Journal of Scholarly Research and Innovation*, *1*(01), 319-350. https://doi.org/10.63125/51kxtf08

[39]. Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of information technology & politics*, *15*(2), 81-93.

[40]. Hsu, C.-L., & Lin, J. C.-C. (2016). Factors affecting the adoption of cloud services in enterprises. *Information Systems and e-Business Management*, *14*(4), 791-822.

[41]. Imtiaz Ferdous, M., Adams, C. A., & Boyce, G. (2019). Institutional drivers of environmental management accounting adoption in public sector water organisations. *Accounting, Auditing & Accountability Journal*, *32*(4), 984-1012.

[42]. Iversen, A.-M., Kavalaris, C. P., Hansen, R., Hansen, M. B., Alexander, R., Kostadinov, K., Holt, J., Kristensen, B., Knudsen, J. D., & Møller, J. K. (2020). Clinical experiences with a new system for automated hand hygiene monitoring: A prospective observational study. *American Journal of Infection Control*, *48*(5), 527-533.

[43]. Kabanda, S., & Brown, I. (2017). A structuration analysis of Small and Medium Enterprise (SME) adoption of E-Commerce: The case of Tanzania. *Telematics and Informatics*, *34*(4), 118-132.

[44]. Kanie, N., Griggs, D., Young, O., Waddell, S., Shrivastava, P., Haas, P. M., Broadgate, W., Gaffney, O., & Kőrösi, C. (2019). Rules to goals: emergence of new governance strategies for sustainable development: Governance for global sustainability is undergoing a major transformation from rule-based to goal-based. But with no compliance measures, success will require an unprecedented level of coherency of action founded on new and reformed institutions nationally and internationally. *Sustainability Science*, *14*(6), 1745-1749.

[45]. Kansal, M., Joshi, M., Babu, S., & Sharma, S. (2018). Reporting of corporate social responsibility in central public sector enterprises: A study of post mandatory regime in India. *Journal of Business Ethics*, *151*(3), 813-831.

[46]. Kauffman, R. J., Ma, D., & Yu, M. (2018). A metrics suite of cloud computing adoption readiness. *Electronic Markets*, *28*(1), 11-37.

[47]. Kompella, L. (2017). E-Governance systems as socio-technical transitions using multi-level perspective with case studies. *Technological Forecasting and Social Change*, *123*, 80-94.

[48]. Krigsholm, P., Riekkinen, K., & Ståhle, P. (2020). Pathways for a future cadastral system: A socio-technical approach. *Land use policy*, *94*, 104504.

[49]. Krishnan, R., Geyskens, I., & Steenkamp, J. B. E. (2016). The effectiveness of contractual and trust-based governance in strategic alliances under behavioral and environmental uncertainty. *Strategic management journal*, *37*(12), 2521-2542.

[50]. Kumar, S., Savur, C., & Sahin, F. (2020). Survey of human–robot collaboration in industrial settings: Awareness, intelligence, and compliance. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(1), 280-297.

[51]. Kutub Uddin, A., Md Mostafizur, R., Afrin Binta, H., & Maniruzzaman, B. (2022). Forecasting Future Investment Value with Machine Learning, Neural Networks, And Ensemble Learning: A Meta-Analytic Study. *Review of Applied Science and Technology*, *1*(02), 01-25. https://doi.org/10.63125/edxgjg56

[52]. Leuz, C., & Wysocki, P. D. (2016). The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research. *Journal of accounting research*, *54*(2), 525-622.

[53]. Li, C., & Palanisamy, B. (2018). Privacy in internet of things: From principles to technologies. *IEEE Internet of Things Journal*, *6*(1), 488-505.

[54]. Li, J., Greenwood, D., & Kassem, M. (2018). Blockchain in the construction sector: A socio-technical systems framework for the construction industry. Advances in Informatics and Computing in Civil and Construction Engineering: Proceedings of the 35th CIB W78 2018 Conference: IT in Design, Construction, and Management,

[55]. Liu, P., Zhou, Y., Zhou, D. K., & Xue, L. (2017). Energy Performance Contract models for the diffusion of green-manufacturing technologies in China: A stakeholder analysis from SMEs' perspective. *Energy Policy*, *106*, 59-67.

[56]. Liverani, M., Teng, S., Le, M. S., & Coker, R. (2018). Sharing public health data and information across borders: lessons from Southeast Asia. *Globalization and health*, *14*(1), 94.

[57]. Lobo, G. J., Neel, M., & Rhodes, A. (2018). Accounting comparability and relative performance evaluation in CEO compensation. *Review of Accounting Studies*, *23*(3), 1137-1176.

[58]. Lu, Y., Xu, X., & Wang, L. (2020). Smart manufacturing process and system automation–a critical review of the standards and envisioned scenarios. *Journal of Manufacturing Systems*, *56*, 312-325.

[59]. Maalek, R., Lichti, D. D., & Ruwanpura, J. Y. (2019). Automatic recognition of common structural elements from point clouds for automated progress monitoring and dimensional quality control in reinforced concrete construction. *Remote Sensing*, *11*(9), 1102.

[60]. Magnusson Sjöberg, C. (2019). Legal automation: AI and law revisited. In *Legal Tech, Smart Contracts and Blockchain* (pp. 173-187). Springer.

[61]. Mansura Akter, E., & Md Abdul Ahad, M. (2022). In Silico drug repurposing for inflammatory diseases: a systematic review of molecular docking and virtual screening studies. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 35-64. https://doi.org/10.63125/j1hbts51

[62]. Mao, H., Zhou, L., Ifft, J., & Ying, R. (2019). Risk preferences, production contracts and technology adoption by broiler farmers in China. *China Economic Review*, *54*, 147-159.

[63]. Martins, R., Oliveira, T., Thomas, M., & Tomás, S. (2019). Firms' continuance intention on SaaS use–an empirical study. *Information Technology & People*, *32*(1), 189-216.

[64]. Md Arifur, R., & Sheratun Noor, J. (2022). A Systematic Literature Review of User-Centric Design In Digital Business Systems: Enhancing Accessibility, Adoption, And Organizational Impact. *Review of Applied Science and Technology*, *1*(04), 01-25. https://doi.org/10.63125/ndjkpm77

[65]. Md Mahamudur Rahaman, S. (2022). Electrical And Mechanical Troubleshooting in Medical And Diagnostic Device Manufacturing: A Systematic Review Of Industry Safety And Performance Protocols. *American Journal of Scholarly Research and Innovation*, *1*(01), 295-318. https://doi.org/10.63125/d68y3590

[66]. Md Nur Hasan, M., Md Musfiqur, R., & Debashish, G. (2022). Strategic Decision-Making in Digital Retail Supply Chains: Harnessing AI-Driven Business Intelligence From Customer Data. *Review of Applied Science and Technology*, *1*(03), 01-31. https://doi.org/10.63125/6a7rpy62

[67]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3d Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[68]. Md Tawfiqul, I., Meherun, N., Mahin, K., & Mahmudur Rahman, M. (2022). Systematic Review of Cybersecurity Threats In IOT Devices Focusing On Risk Vectors Vulnerabilities And Mitigation Strategies. *American Journal of Scholarly Research and Innovation*, *1*(01), 108-136. https://doi.org/10.63125/wh17mf19

[69]. Mechler, R. (2016). Reviewing estimates of the economic efficiency of disaster risk management: opportunities and limitations of using risk-based cost–benefit analysis. *Natural Hazards*, *81*(3), 2121-2147.

[70]. Medeiros, E. (2019). Cross-border transports and cross-border mobility in EU border regions. *Case studies on transport policy*, *7*(1), 1-12.

[71]. Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45.

[72]. Mirkovski, K., Davison, R. M., & Martinsons, M. G. (2019). The effects of trust and distrust on ICT-enabled information sharing in supply chains: Evidence from small-and medium-sized enterprises in two developing economies. *The International Journal of Logistics Management*, *30*(3), 892-926.

[73]. Mirkovski, K., Lowry, P. B., & Feng, B. (2016). Factors that influence interorganizational use of information and communications technology in relationship-based supply chains: evidence from the Macedonian and American wine industries. *Supply Chain Management: An International Journal*, *21*(3), 334-351.

[74]. Mohtaramzadeh, M., Ramayah, T., & Jun-Hwa, C. (2018). B2B e-commerce adoption in Iranian manufacturing companies: Analyzing the moderating role of organizational culture. *International Journal of Human–Computer Interaction*, *34*(7), 621-639.

[75]. Naujoks, F., Wiedemann, K., Schömig, N., Hergeth, S., & Keinath, A. (2019). Towards guidelines and verification methods for automated vehicle HMIs. *Transportation research part F: traffic psychology and behaviour*, *60*, 121-136.

[76]. Oulasvirta, L., & Anttiroiko, A.-V. (2017). Adoption of comprehensive risk management in local government. *Local Government Studies*, *43*(3), 451-474.

[77]. Pagallo, U., Corrales, M., Fenwick, M., & Forgó, N. (2018). The rise of robotics & AI: technological advances & normative dilemmas. *Robotics, AI and the Future of Law*, 1-13.

[78]. Park, H., & Kim, J. D. (2020). Transition towards green banking: role of financial regulators and financial institutions. *Asian Journal of Sustainability and Social Responsibility*, *5*(1), 1-25.

[79]. Pitt, J., Diaconescu, A., & Ober, J. (2018). Knowledge management for democratic governance of socio-technical systems. In *The Future of Digital Democracy: An Interdisciplinary Approach* (pp. 38-61). Springer.

[80]. Proskurina¹, N. (2019). Socio-Technical Approach to a Research. *Digital Age: Chances, Challenges and Future*, *84*, 458.

[81]. Raghupathi, V., Zhou, Y., & Raghupathi, W. (2018). Legal decision support: exploring big data analytics approach to modeling pharma patent validity cases. *IEEE Access*, *6*, 41518-41528.

[82]. Ranchordás, S., & Goanta, C. (2020). The new city regulators: Platform and public values in smart and sharing cities. *Computer law & security review*, *36*, 105375.

[83]. Rao, R. N., & Sridhar, B. (2018). IoT based smart crop-field monitoring and automation irrigation system. 2018 2nd International Conference on Inventive Systems and Control (ICISC),

[84]. Reduanul, H., & Mohammad Shoeb, A. (2022). Advancing ai in marketing through cross border integration ethical considerations and policy implications. *American Journal of Scholarly Research and Innovation*, *1*(01), 351-379. https://doi.org/10.63125/d1xg3784

[85]. Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems*, *20*, 26-37.

[86]. Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer law & security review*, *34*(1), 99-110.

[87]. Rose, C. (2016). Firm performance and comply or explain disclosure in corporate governance. *European Management Journal*, *34*(3), 202-222.

[88]. Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, *7*, 50759-50779.

[89]. Sadok, M., Welch, C., & Bednar, P. (2020). A socio-technical perspective to counter cyber-enabled industrial espionage. *Security Journal*, *33*(1), 27-42.

[90]. Sanz, J. L., & Zhu, Y. (2021). Toward scalable artificial intelligence in finance. 2021 IEEE International Conference on Services Computing (SCC),

[91]. Sazzad, I., & Md Nazrul Islam, K. (2022). Project impact assessment frameworks in nonprofit development: a review of case studies from south asia. *American Journal of Scholarly Research and Innovation*, *1*(01), 270-294. https://doi.org/10.63125/eeja0t77

[92]. Simbeck, K. (2019). HR analytics and ethics. *IBM Journal of Research and Development*, *63*(4/5), 9: 1-9: 12.

[93]. Sluis, S., & De Giovanni, P. (2016). The selection of contracts in supply chains: An empirical analysis. *Journal of Operations Management*, *41*, 1-11.

[94]. Smallwood, R., Kahn, R. E., & Murphy, B. (2012). Information Governance and Legal Functions. *Information Governance: Concepts, Strategies and Best Practices*, 115-145.

[95]. Sohel, R., & Md, A. (2022). A Comprehensive Systematic Literature Review on Perovskite Solar Cells: Advancements, Efficiency Optimization, And Commercialization Potential For Next-Generation Photovoltaics. *American Journal of Scholarly Research and Innovation*, *1*(01), 137-185. https://doi.org/10.63125/843z2648

[96]. Stella, B., & Bwalya, K. J. (2018). Fog computing in a developing world context: Jumping on the bandwagon. In *Fog Computing: Concepts, Frameworks and Technologies* (pp. 63-80). Springer.

[97]. Subrato, S. (2018). Resident's Awareness Towards Sustainable Tourism for Ecotourism Destination in Sundarban Forest, Bangladesh. *Pacific International Journal*, *1*(1), 32-45. https://doi.org/10.55014/pij.v1i1.38

[98]. Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer law & security review*, *35*(4), 380-397.

[99]. Taal, A., Sherer, J. A., Bent, K.-A., & Fedeles, E. R. (2016). Cognitive computing and proposed approaches to conceptual organization of case law knowledge bases: a proposed model for information preparation, indexing, and analysis. *Artificial Intelligence and Law*, *24*(4), 347-370.

[100]. Tahmina Akter, R., & Abdur Razzak, C. (2022). The Role Of Artificial Intelligence In Vendor Performance Evaluation Within Digital Retail Supply Chains: A Review Of Strategic Decision-Making Models. *American Journal of Scholarly Research and Innovation*, *1*(01), 220-248. https://doi.org/10.63125/96jj3j86

[101]. Taylor, R. D. (2020). "Data localization": The Internet in the balance. *Telecommunications Policy*, *44*(8), 102003.

[102]. Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A. (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer law & security review*, *34*(3), 582-594.

[103]. Unsworth, R. (2019). Smart contract this! An assessment of the contractual landscape and the Herculean challenges it currently presents for "Self-executing" contracts. In *Legal tech, smart contracts and blockchain* (pp. 17-61). Springer.

[104]. Van Der Sype, Y. S., & Maalej, W. (2014). On lawful disclosure of personal user data: What should app developers do? 2014 IEEE 7th International Workshop on Requirements Engineering and Law (RELAW),

[105]. Vroege, W., Dalhaus, T., & Finger, R. (2019). Index insurances for grasslands–A review for Europe and North-America. *Agricultural systems*, *168*, 101-111.

[106]. Wu, C.-C. (2016). Status quo bias in information system adoption: a meta-analytic review. *Online Information Review*, *40*(7), 998-1017.

[107]. Yeh, C.-L. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, *42*(4), 282-292.

[108]. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & governance*, *12*(4), 505-523.

[109]. You, J., Chen, Y., Wang, W., & Shi, C. (2018). Uncertainty, opportunistic behavior, and governance in construction projects: The efficacy of contracts. *International journal of project management*, *36*(5), 795-807.

[110]. Zekos, G. I. (2021). AI and legal issues. In *Economics and Law of Artificial Intelligence: Finance, Economic Impacts, Risk Management and Governance* (pp. 401-460). Springer.

[111]. Zhong, B., Gan, C., Luo, H., & Xing, X. (2018). Ontology-based framework for building environmental monitoring and compliance checking under BIM environment. *Building and Environment*, *141*, 127-142.

[112]. Zhu, L., Wu, Y., Gai, K., & Choo, K.-K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, *91*, 527-535.