Science of Law Journal (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2025.040514
ISSN 2616-2296 Vol. 4 Num. 5

Investigating Data-Driven Strategies for Intelligent Compliance and Risk Management in Enterprises from a Legal-Business Integration Perspective

Jun Zhao

Missouri State University Springfield, MO 65897, USA

Keywords: Legal-Commercial Integration; Data-Driven; Corporate Intelligence Compliance and Risk Management

Abstract: As the pace of global digitalisation accelerates, enterprises face increasingly complex compliance environments and risks. According to Deloitte's 2024 Global Compliance and Risk Trends Report, over 76% of organisations reported experiencing significant operational disruption or financial loss within the past three years due to compliance failures. Traditional risk management models reliant on manual processes and experience demonstrate shortcomings in efficiency, precision, and foresight. The integration of law and business organically combines legal and commercial knowledge systems, offering fresh perspectives and approaches to corporate compliance and risk management. Data-driven methodologies leverage advanced technologies such as big data and artificial intelligence to collect, analysis', and mine vast datasets generated during business operations. This enables precise identification, assessment, and prediction of risks, providing scientific and objective foundations for corporate compliance and risk management. Therefore, this paper, grounded in the integration of law and business, explores how to deeply merge the bottom-line thinking of legal compliance with the value creation demands of business management. It systematically utilises data-driven technologies such as big data and artificial intelligence to construct an intelligent, adaptive, and forward-looking corporate compliance and risk management framework. This aims to provide theoretical reference and practical guidance for enterprises seeking steady and innovative development in the digital economy era.

1. Introduction

At present, the digital economy has become a new engine for global economic growth. According to IDC projections, the total volume of data generated worldwide is expected to reach 221 zettabytes by 2026, with China's digital economy anticipated to exceed 120 trillion yuan. The operational environment for enterprises is undergoing profound transformation. The market-driven allocation of data as a key resource, the rapid proliferation of global regulatory frameworks, and the accelerated evolution of business models have expanded the boundaries of corporate compliance and risk management beyond traditional finance and legal domains. These now encompass emerging areas such as data privacy, algorithmic ethics, cybersecurity, and supply chain resilience. Conventional risk

management approaches struggle to address this increasingly complex and dynamic business landscape. The integration of law and business necessitates that enterprises dismantle barriers between legal and operational functions, transforming compliance requirements from cost centres into value centres that generate competitive advantages. The maturation of data-driven technological paradigms now enables enterprises to transition risk management from experience-driven approaches to data intelligence-driven methodologies. Consequently, this study endeavours to systematically construct an intelligent compliance and risk management framework for enterprises that integrates legal-business thinking and is profoundly empowered by data technology, thereby providing practical guidance for corporate implementation[1].

2. The Coupling Relationship between Legal-Commercial Integration and Data-Driven Approaches

2.1 The Essence and Value of Legal-Commercial Integration

Legal-commercial integration is not merely the simple juxtaposition of law and commerce, but rather a profound, systematic mindset and governance philosophy. Research by the BM Commercial Value Institute, surveying 1,200 senior executives globally, indicates that enterprises adopting a "legal-commercial integration" mindset achieve a 28% higher success rate in digital projects compared to their peers, while reducing the average resolution time for compliance-related disputes by 50%.The "legal" dimension emphasises rule compliance, rights protection, and bottom-line thinking, ensuring corporate conduct operates within lawful boundaries and mitigating disruptive risks. The "business" aspect prioritises efficiency optimisation, value creation, and innovation-driven growth, pursuing continuous enhancement of core competitiveness. The core value of legal-business integration lies in guiding enterprises to proactively seek the greatest common denominator between compliance thresholds and commercial objectives in strategic planning and daily operations. For instance, in data development and utilisation, it entails adhering to privacy protection regulations while simultaneously extracting commercial value from data, thereby maximising the worth of data assets within a compliant framework[2].

2.2 Data-Driven Technical Systems and Capability Support

Data-driven approaches provide the foundational infrastructure for intelligent compliance and risk management. Firstly, they offer panoramic data perception capabilities. Enterprises can utilise technologies such as big data platforms to comprehensively and exhaustively collect and aggregate risk-related data from internal and external sources, diverse origins, and varied structures. Secondly, they possess intelligent analytical and predictive capabilities. Enterprises can utilise artificial intelligence to conduct deep mining of aggregated data, thereby discerning potential risk patterns, trends, and developmental trajectories from vast information pools, shifting from reactive post-event responses to proactive pre-event warnings. Thirdly, data-driven approaches possess automated response capabilities. Upon identifying specific risks or compliance triggers through intelligent analysis, this capability automatically executes standardised compliance checks, risk controls, or report generation via predefined rules and process engines. This replaces repetitive manual operations, significantly enhancing efficiency while reducing human error[3]. Fourthly, data-driven approaches possess knowledge graph construction capabilities. Organisations can employ graph computing technologies to interconnect fragmented knowledge elements—such as regulatory provisions, judicial precedents, internal operational rules, and entity relationships—forming an interconnected semantic network. This provides deep, inferential contextual knowledge support for risk analysis, prediction, and automated decision-making. Ultimately, these capabilities collectively empower enterprises to

establish an intelligent compliance and risk management system characterised by comprehensive perception, intelligent analysis, precise decision-making, and efficient execution.

2.3 The Coupling Mechanism of Legal-Commercial Integration and Data-Driven Approaches

Legal-commercial integration and data-driven methodologies are mutually reinforcing, collectively forming the core and driving force of intelligent compliance and risk management systems. Data-driven approaches serve as the enabling engine for legal-commercial integration, transforming abstract legal provisions and complex commercial logic into quantifiable, computable data models. This facilitates the transition of legal-commercial integration from conceptual framework to executable, measurable practice. For instance, Natural Language Processing (NLP) technology parses ever-evolving regulatory policies, converting them into structured tags recognisable by IT systems. This achieves the digitisation and codification of regulations. Legal-business integration serves as a data-driven compass for value, ensuring that data technology applications consistently align with corporate strategic objectives and compliance thresholds, thereby preventing misuse or deviation from core business principles. For instance, when developing customer credit risk models, this integrated approach demands not only predictive accuracy but also compliance with financial regulatory requirements for fairness and transparency.(as shown in Figure 1)

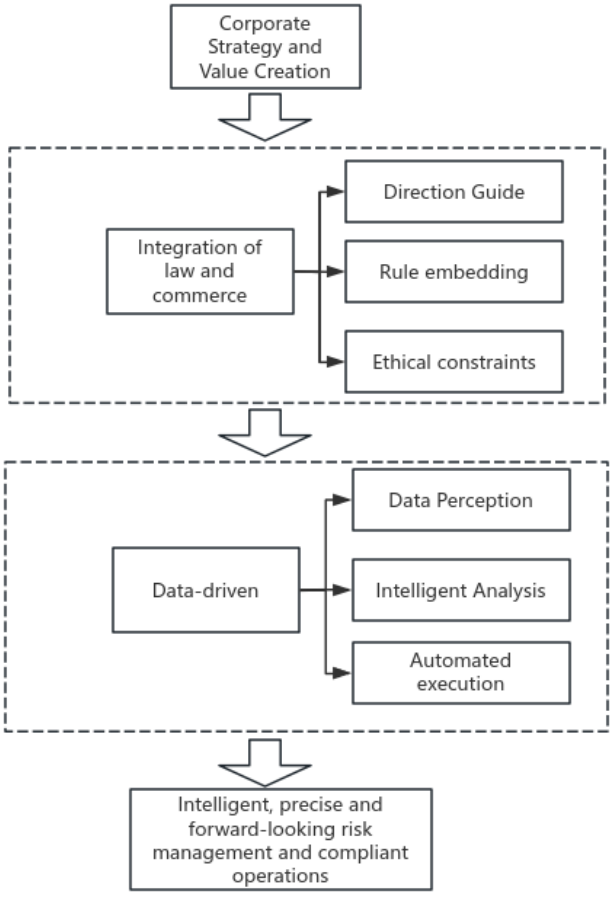

Figure 1: Coupling Relationship Model between Legal-Commercial Integration and Data-Driven Approaches

3. Data-Driven Enterprise Intelligence Compliance and Risk' Management Framework

3.1 Compliance and Risk Management Framework Supported by Data Layer, Intelligence Layer, and Application Layer

The data layer serves as the foundation of the entire system, with its core task being to address the origins of data and its governance, achieving comprehensive and standardised aggregation of risk data. It breaks down departmental silos by aggregating structured and unstructured data from systems including ERP, CRM, SCM, OA, financial systems, IT system logs, and internal whistleblowing platforms. This data reflects the true pulse of enterprise operations. It also extensively integrates external data sources such as regulatory databases, judicial case repositories, public sentiment data, supply chain information, and industry risk intelligence. Furthermore, raw data must undergo governance to generate value. The data layer establishes a unified risk data lake, performing cleansing, labelling, integration, and structuring of multi-source heterogeneous data. Crucially, it employs natural language processing to convert unstructured regulatory texts and contracts into machine-readable, comprehensible structured information, supplying high-quality, reusable data fuel for upper-layer intelligent applications[4].

The intelligence layer constitutes the framework's core, employing advanced algorithmic models to perform deep processing on data-layer insights, achieving the leap from data to actionable intelligence. Primarily relying on unsupervised and supervised learning algorithms, it autonomously identifies anomalous patterns and outliers within vast transaction and log data without prior labelling, enabling detection of unknown fraud, internal threats, and similar risks. It can train models using historical risk case data to precisely identify known risk types, such as money laundering transaction detection and fraudulent invoice identification. Furthermore, it employs NLP models to deeply comprehend the semantics of laws, regulations, supervisory requirements, and internal policies, decomposing them into specific compliance clauses and rules. Subsequently, the rules engine automatically compares these rules against real-time incoming business data, generating immediate compliance deviation alerts to achieve compliance-as-code.

The application layer serves as the interface where intelligent analysis results interact with end-users, transforming abstract intelligence into tangible productivity. The intelligent contract review system provides automated contract review services for legal and business personnel, identifying critical risk clauses, omissions of rights and responsibilities, and comparing against standard templates within seconds; It furnishes managers with an enterprise-wide risk overview, visually presenting various risk metrics, alert events, and geographical distributions in real time, enabling ‘single-screen awareness.’ It also replaces manual labour in repetitive, standardised compliance tasks, such as automated regulatory reporting, 24-hour anti-money laundering transaction monitoring, and automated spot checks on employee behavioural compliance.

3.2 Data-Driven Transformation of Core Enterprise Risk Management Processes

The effective operation of a compliance and risk management framework underpinned by data, intelligence, and application layers transcends mere technological aggregation. It catalyses profound transformation within core enterprise risk management processes, as illustrated in the comparative table below (Table 1).

This framework systematically addresses the critical question of how to integrate legal and commercial integration principles with data-driven technology implementation. It achieves digitalisation of risk perception through the data layer, enables intelligent risk analysis via the intelligence layer, and ultimately delivers scenario-based and operationalised risk management through the application layer. This framework is not merely a technical solution but represents a novel

management paradigm. Through profound process re-engineering, it propels corporate compliance and risk management from being a cost centre towards becoming a value-creating hub, laying a solid foundation for enterprises to navigate steadily and achieve long-term success in complex and volatile environments[5].

Table 1: The fundamental shift in risk management paradigms

Traditional management paradigm	Intelligent Management Paradigm	The Transformation Achieved by This Framework
Remedial action	Pre-emptive alerts and in-process intervention	Enterprises utilise predictive models and real-time monitoring to issue early warnings before or at the onset of risk events, thereby significantly advancing the management frontline.
Static compliance	Dynamic monitoring and adaptive response	The system continuously monitors changes in external regulatory policies, automatically analysing their alignment with internal operational procedures and triggering necessary update processes.
Siloed management	Collaborative governance and closed-loop management	The framework unifies data, models, and processes. A risk event identified at the business end automatically triggers investigations by risk control, assessments by legal, and follow-up by audit.
Experience-driven	Data-driven	Decision-making no longer relies solely on the experience-based judgements of individuals or teams, but is grounded in objective evidence derived from comprehensive data analysis and model outputs.

4. Exploring Data-Driven Enterprise Intelligence for Compliance and Risk Management Strategies

4.1 Data Intelligence-Based Risk Identification and Assessment

Data intelligence-based risk 'dentification and assessment strategies utilise data models to replace manual expertise, achieving automated, precise and forward-looking risk insights. This shifts risk management focus from post-event investigation to pre-emptive warning and real-time detection. Traditional risk identification relies on overt risk signals, whereas the data-driven approach constructs a multidimensional data perception network to detect emerging risks early from vast volumes of weak signals. It encompasses not only internal financial data but also behavioural data, relational data, and textual data. For instance, in anti-commercial bribery scenarios, the system concurrently analyses: reimbursement amounts, frequency, and supplier concentration, whether employee travel timings align with business cycles, abnormal acceleration in approval workflows, unusual connections between employees and suppliers, corruption-related negative publicity concerning partners.

4.2 Automated Compliance Controls Integrated into Business Processes

The core of automated compliance controls integrated into business processes is “compliance as code”. This transforms compliance requirements from external, textual regulations into rules embedded within business processes for automatic execution. It shifts controls upstream, moving from post-event correction to real-time interception. By translating compliance logic into rules or models that computers can understand and execute, and embedding these into critical business

process systems, compliance verification occurs instantaneously during business operations. For instance, during intelligent contract review, within an enterprise's electronic contract approval workflow, when a business user uploads a draft contract, the system automatically invokes an NLP compliance engine. This engine performs deep semantic analysis on the contract text, conducting multi-dimensional comparisons against an embedded repository of standard contract templates, a regulatory knowledge base, and internal company policies. The system automatically flags potentially risky clauses while directly providing amendment suggestions and regulatory references. This not only liberates legal professionals from burdensome preliminary review tasks—boosting review efficiency by over 80%—but crucially enables business personnel to perceive compliance requirements during the drafting stage, thereby enhancing organisational-wide compliance awareness(as shown in Figure 2).

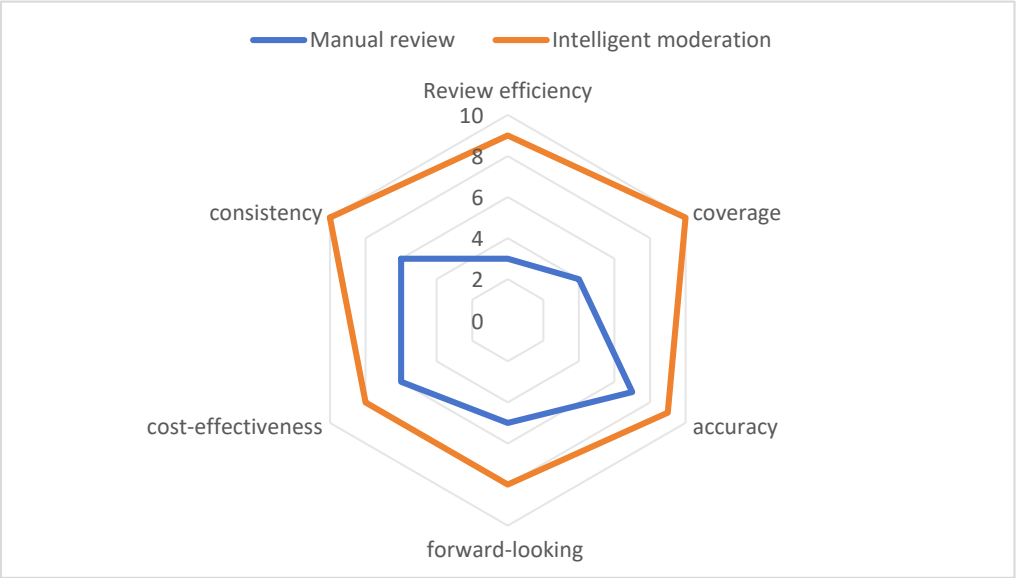

Figure 2 Contract Review Capability Dimension Assessment Form

4.3 Scenario-Oriented Intelligent Decision Support and Response Strategies

Scenario-oriented intelligent decision support and response strategies address increasingly complex, non-standardised scenarios. They provide managers with panoramic data insights and simulation capabilities for strategic decision-making and emergency response to unforeseen events, elevating risk management from mere control to an enabler of informed decision-making. Leveraging technologies such as knowledge graphs and simulation modelling, it constructs a digital twin within a virtual environment that mirrors real-world operational conditions. This enables managers to comprehensively evaluate potential risks and compliance implications across different scenarios prior to decision-making. When a company plans to enter a new national market, managers input the target market name into the system. Based on the knowledge graph, the system automatically generates a Panoramic Risk Insight Report. This report visually presents key requirements and enforcement rigor of the region's data protection, labour, environmental, and tax laws. It correlates major competitors' litigation histories and intellectual property portfolios within the region, analyses their common competitive strategies and potential risks, displays risk profiles of prospective agents and suppliers, and reveals underlying equity structures and collaborative networks. Managers gain a systematic risk overview that transcends individual experience and fragmented research. This enables them to proactively avoid high-risk areas when formulating market entry strategies, select more reliable partners, and make more informed decisions.

5. Implementation and Safeguards for Enterprises in Establishing Data-Driven Intelligent Compliance and Risk Management Systems

5.1 Phased Implementation to Solidify Foundations

Establishing a data-driven intelligent compliance and risk management system is a complex systemic undertaking that cannot be achieved overnight. Enterprises should adopt a three-stage evolutionary strategy tailored to their current circumstances, progressing from simpler to more complex tasks and expanding from specific points to comprehensive coverage. At the initial stage, enterprises may establish a Data Governance Committee to formulate unified data standards, quality rules, and security management protocols. This article prioritizes integrating data from core departments such as legal affairs, risk management, finance, and auditing. Develop a theme-centered risk data model to form an initial risk data warehouse, thereby increasing the risk data coverage rate from less than 30% to 70%. In the intermediate stage, organisations should introduce or develop AI tools in areas with robust data foundations and acute operational pain points. We will give priority to the human-machine collaboration model, with artificial intelligence conducting the initial screening and recommendation, and experts making the final judgment. This approach reduces transformation resistance and accumulates annotated data. Meanwhile, this paper breaks down departmental silos by establishing a joint intelligent risk control project team composed of representatives from the legal, risk management, IT and business departments. The implementation of standardized communication, decision-making and problem-solving mechanisms has increased the efficiency of risk identification by 50%. At the advanced stage, enterprises should consolidate and refine the dispersed AI capabilities and data services developed during the intermediate phase. This forms a unified, reusable intelligent middle platform capable of rapidly delivering standardised risk identification, assessment, and control services to any business scenario across the organisation. Furthermore, enterprises should incorporate key suppliers, distributors, and partners into a unified risk monitoring network via secure API interfaces and data exchange protocols. This enables real-time perception and collaborative management of external ecosystem risks, boosting enterprise-wide risk response speed by 60% and achieving interconnected risk data with 80% of core partners.

5.2 Providing Comprehensive Safeguards to Facilitate Corporate Transformation

Corporate transformation is a top-level initiative. Research by the World Bank indicates that enterprises where digital transformation is directly spearheaded by the CEO or board achieve project success rates 2.5 times higher than other organisations. The board and senior management must explicitly articulate their support and establish a clear governance structure (As shown in Figure 3)

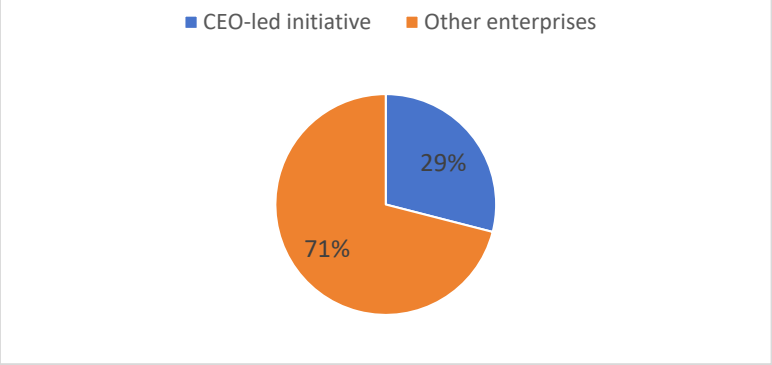

Figure 3 Comparison of Digital Transformation Success Rates

The board bears ultimate responsibility, the chief executive drives implementation, a chief compliance officer with substantive authority is appointed, and a cross-departmental risk management committee is formed. Building upon this foundation, enterprises must cultivate a corporate culture centred on data-driven decision-making, proactive risk management, and shared accountability through continuous training, awareness campaigns, and incentive mechanisms. Employees should understand that intelligent risk management is not surveillance, but empowerment and protection, encouraging proactive reporting of risk incidents rather than concealment. Concurrently, organisations should invest in stable, secure, and highly available cloud-native architectures to ensure systems can handle massive data processing and high-concurrency access. Technology selection should prioritise openness and interoperability to prevent new data silos. We have established a governance framework covering the entire data lifecycle - from collection, storage, processing and analysis to application and destruction - to prevent low-quality data from entering the system and generating defective insights by defining data ownership, implementing data quality monitoring and establishing accountability mechanisms. Furthermore, organisations must recognise the potential for black-box issues and algorithmic bias within AI models. Consequently, they should conduct regular third-party audits of core risk models to verify fairness, accuracy, and stability. A clear accountability framework must be established to enable traceability to specific individuals when automated decisions result in adverse impacts.

6. Conclusion

Data-driven corporate intelligence compliance and risk management through the lens of legal-business integration represents an inevitable choice for enterprises seeking sustainable development in the digital age. This innovative model not only assists businesses in effectively navigating increasingly complex legal regulations and supervisory requirements, thereby mitigating legal risks and economic losses, but also enhances operational efficiency and market competitiveness while strengthening corporate social responsibility and credibility. With continuous technological advancement and expanding applications, this field demonstrates vast developmental prospects. Enterprises should proactively embrace this trend, taking initiative to strengthen the practical application of legal-business integration and data-driven approaches. This research continuously improves the data governance system by strengthening data standardization, quality control and security guarantee, ensuring the accuracy, completeness and security of data, and providing a high-quality data foundation for intelligent compliance and risk management. Optimize the functions and performance of the intelligent compliance platform, customize compliance solutions to align with business characteristics and requirements, thereby enhancing the efficiency and effectiveness of compliance management. The theoretical framework and strategic system outlined herein aims to provide enterprises with a viable pathway from conceptualisation to implementation. This system can significantly enhance an organisation's risk resilience and compliance efficiency, transforming compliance from a passive burden into an active value-creating activity. Ultimately, it builds the core competitive advantage essential for sustainable, high-quality enterprise development.

References

[1] Hong Tao. The Enabling Logic, Legal Risks an' Governance Responses of Compliance Technology in the Digital Era [J]. China Science and Technology Forum, 2025(6):1-9.

[2] Xu Xuesong, Yang Wanlian, Guan Min, et al. Financial Technology Innovation and Risk Management Transformation in China's Digital Economy Era [J]. China Engineering Science, 2025(3).

[3] Cheng Chao, Gong Weishuai, Cui Xiwei, et al. Building a Digital-Intelligent Power Marketing System Driving Full-Chain Compliance Management [J]. Enterprise World, 2024(20):76-80.

[4] Tao Zhenzhen, Zhang Yanshu. Constructing a Three-Tier Financial Risk Management System for 'Enterprise-

Department-Individual' Driven by Digital Technology [J]. Accounting and Finance Bulletin, 2025(10).
[5] Chen Tong. Financial Management Challenges and Transformation Pathways for E-commerce Enterprises in the Digital Economy Era: A Case Study of Alibaba Group [J]. E-Commerce Review, 2025, 14(8):5.