Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Operationalising AI Legal Governance: A Regulatory Compliance Framework for AI Systems.

Article History:

Name of Author:
Professor Bernard Wong.

Affiliation:
Enterprise Strategy Consulting Inc, Sydney, Australia.

Corresponding Author:
Professor Bernard Wong.

How to cite this article:
Wong B. Operationalising AI legal governance: A regulatory compliance framework for AI systems. Professor Bernard Wong. *J Int Commer Law Technol.* 2026; 7(1):1374–1384.

Received: *06-03-2026*
Revised: *08-04-2026*
Accepted: *29-04-2026*
Published: *07-05-2026*

Abstract: The rapid adoption of Artificial Intelligence (AI) across commercial and public sectors has introduced significant legal and regulatory challenges, particularly in relation to accountability, liability, data protection, and algorithmic transparency. While existing governance frameworks, including the NIST Artificial Intelligence Risk Management Framework and ISO/IEC 42001, provide structured approaches to risk management, they do not fully operationalise legal compliance within organisational practice. This paper addresses this gap by developing a six-phase AI legal governance framework that integrates regulatory requirements, including the EU Artificial Intelligence Act, data protection law, and emerging international standards, into organisational processes. Using an integrative synthesis of legal, regulatory, and governance literature, the study identifies persistent fragmentation between ethical principles, technical controls, and enforceable legal obligations. The proposed framework operationalises legal compliance through structured phases encompassing legal and regulatory alignment, risk classification, compliance-by-design, organisational capability development, continuous legal auditing, and regulatory assurance. It provides organisations with a practical mechanism to mitigate legal risk, ensure regulatory compliance, and enhance accountability in AI deployment. This study contributes to the field of commercial law and technology by bridging the gap between regulatory principles and organisational implementation, offering a legally grounded model for responsible and enforceable AI governance.

Keywords: Artificial Intelligence (AI); AI legal governance; regulatory compliance; EU Artificial Intelligence Act; data protection law; algorithmic accountability; legal liability; automated decision-making; consumer protection law; misrepresentation; ISO/IEC 42001; NIST AI Risk Management Framework.

INTRODUCTION

Artificial Intelligence (AI) is transforming organisational operations and strategic decision-making across all sectors, yet its rapid diffusion has outpaced the development of effective governance mechanisms. As AI systems become embedded in critical domains such as finance, healthcare, public services, and human resources, organisations face mounting challenges related to accountability, transparency, fairness, and compliance. These challenges extend beyond technological risk to encompass legal, ethical, and societal implications that threaten public trust and corporate legitimacy if not properly governed.

While numerous ethical guidelines and regulatory initiatives, such as the OECD AI Principles [1], the EU AI Act [2], and the NIST AI Risk Management Framework (AI RMF 1.0) [3], seek to promote responsible AI, translating these high-level principles into actionable governance processes remains an enduring gap. Existing frameworks often emphasise either compliance or technical risk management but fail to integrate strategic, ethical, and legal perspectives within a coherent organisational model. Consequently, many organisations continue to struggle with operationalising responsible AI in a way that aligns with their corporate strategy, regulatory obligations, and stakeholder expectations.

The governance of Artificial Intelligence is increasingly a matter of legal compliance rather than voluntary ethical practice. Emerging regulatory frameworks, particularly the EU Artificial Intelligence Act, impose binding obligations on organisations deploying high-risk AI systems, including requirements for transparency, documentation, human oversight, and risk management. Similarly, existing legal regimes such as data protection law, consumer protection law, and contractual liability frameworks are being applied to AI-enabled systems. As a result, organisations face growing exposure to legal liability arising from algorithmic bias, unlawful data processing, automated decision-making, and system failures.

Recent systematic reviews of AI governance literature (e.g., Birkstedt et al. [4]; Batool et al. [5]) highlight four persistent challenges: the absence of unified governance frameworks, limited empirical evidence on implementation effectiveness, fragmentation between ethical and legal controls, and inadequate cross-functional accountability. These shortcomings underline the urgent need for governance structures that can bridge the gap between principle and practice, ensuring that AI adoption enhances rather than undermines ethical conduct, regulatory compliance, and organisational resilience.

This paper addresses this gap by proposing a six-phase AI Legal Governance Framework. Drawing upon multi-industry analyses and leading international standards, including the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) [3], ISO/IEC 42001 [6], and the EU Artificial Intelligence Act [2], as well as governance guidance from the Australian Institute of Company Directors (AICD) [8], the framework integrates procedural, risk-based, governance, and legal dimensions of AI oversight. It builds upon the insights of Roppelt et al. [7] and incorporates Wong's legal risk governance recommendations [9] to embed regulatory compliance, accountability, and liability management across the AI lifecycle. The framework operationalises key principles, including fairness auditing, privacy-by-design, accountability, and cross-functional oversight, into actionable governance processes.

By reframing AI governance as a matter of enforceable legal compliance rather than voluntary ethical practice, this study contributes to the field of commercial law and technology. It provides organisations with a structured and legally grounded framework for aligning AI deployment with regulatory obligations, managing liability risks, and ensuring accountability. In doing so, it offers a practical roadmap for embedding legal governance within organisational systems, supporting transparent, compliant, and sustainable AI adoption.

RESEARCH METHODOLOGY

This study employs a qualitative integrative synthesis of secondary data drawn from peer-reviewed research, international governance frameworks, and institutional reports on Artificial Intelligence (AI) governance and adoption. Rather than collecting new empirical data, the analysis consolidates findings from multiple authoritative sources to derive a comprehensive legal governance framework that integrates strategic, ethical, and legal dimensions of responsible AI. The synthesis aligns with the interpretive logic of systematic literature reviews and framework integration studies (e.g., Birkstedt et al. [4]; Batool et al. [5]), combining conceptual mapping and cross-framework comparison to develop a practical model of responsible AI governance.

Scope of Data Sources

The synthesis draws upon:

1. Peer-reviewed empirical studies examining AI adoption and governance across industries, including Roppelt et al. [7] on talent acquisition, Atwal et al. [10] on strategic adoption, and Jhansi Rani et al. [11] on AI in HR transformation.
2. International regulatory and standards frameworks, notably the NIST AI Risk Management Framework (AI RMF 1.0) [3], ISO/IEC 42001 [6], and the EU AI Act [2], which collectively define global expectations for risk-based AI governance.
3. Scholarly syntheses and conceptual analyses such as Birkstedt et al. [4] and Wong [9], which articulate ethical, legal, and organisational gaps in current AI governance practices.

These sources were selected based on their academic credibility, recency (2021–2025), and relevance to AI governance mechanisms, risk management, and ethical accountability.

Analytical Process

The synthesis followed a three-stage analytical

process:

1. Extraction and Coding: Each source was reviewed to identify recurring governance mechanisms, including accountability structures, auditing processes, risk controls, and ethical design principles.
2. Cross-Framework Comparison: The identified mechanisms were compared across studies and standards to determine convergence and divergence between strategic, ethical, and regulatory perspectives.
3. Integration and Model Development: Insights were synthesized to construct a six-phase AI Legal Governance Framework, integrating procedural steps from Roppelt et al. [7], risk-centric controls from the NIST AI RMF 1.0 [3], and legal-ethical governance principles from Wong [9].

This integrative synthesis ensures that the proposed framework is grounded in established theory while addressing the fragmentation and operationalisation gaps identified in recent systematic reviews (e.g., Birkstedt et al. [4]; Batool et al. [5]).

Rationale for the Integrative Approach

A synthesis-based methodology is appropriate for the present research objective because it enables the consolidation of multi-disciplinary insights into a unified, actionable model. The complexity of AI governance, spanning technical, ethical, and legal domains, requires integration across academic and regulatory sources rather than isolated empirical observation. By systematically mapping and integrating these perspectives, this study advances a structured roadmap that organisations can adapt to ensure responsible, transparent, and legally compliant AI deployment.

LEGAL AND REGULATORY CHALLENGES IN AI DEPLOYMENT

The deployment of Artificial Intelligence (AI) systems raises a series of complex legal issues that engage multiple areas of commercial and public law, including data protection, liability, anti-discrimination, and consumer protection. These challenges are not merely theoretical but reflect an emerging body of regulatory practice and judicial consideration concerning the legal accountability of automated systems.

First, AI deployment frequently involves the large-scale processing of personal data, thereby engaging data protection regimes such as Australia's Privacy Act 1988 [12] and the General Data Protection Regulation (GDPR) [13]. Under Article 22 of the GDPR, individuals have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. This provision imposes obligations of transparency, explainability, and human oversight. Judicial interpretation has reinforced these principles; in Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos, the Court of Justice of the European Union (CJEU) emphasised the importance of protecting individual rights in the context of automated data processing [14]. Similarly, regulatory guidance has underscored that opaque algorithmic systems may breach fundamental data protection principles where meaningful explanation cannot be provided.

Second, the question of liability for AI-generated outcomes remains unsettled within existing legal frameworks. Traditional doctrines of negligence and product liability are challenged by the autonomous and adaptive nature of AI systems. In Donoghue v Stevenson [15], the foundational principle of duty of care established that manufacturers owe obligations to end users; however, its application to AI systems, particularly those that evolve post-deployment, raises questions regarding foreseeability and control. More recent developments, including proposals within the EU regulatory framework, suggest that liability may increasingly be assigned to deployers of high-risk AI systems, reflecting a shift toward risk-based accountability. The absence of clear judicial precedent in this area underscores the importance of embedding legal compliance mechanisms within organisational governance structures.

Third, algorithmic bias and discriminatory outcomes present significant legal risks under anti-discrimination law. AI systems used in recruitment, credit scoring, or service delivery may inadvertently replicate or amplify existing biases, resulting in unlawful discrimination. In Lloyd v Google LLC [16], although primarily a data protection case, the UK Supreme Court highlighted the broader implications of large-scale data misuse and the challenges of establishing individual harm. Regulatory authorities have increasingly signalled that organisations deploying AI systems bear responsibility for ensuring that outcomes do not contravene equality legislation, thereby necessitating proactive bias auditing and monitoring.

Fourth, AI deployment introduces risks within the domain of contract and consumer protection law. Where AI-generated outputs are relied upon in commercial transactions, inaccurate or misleading information may give rise to claims for misrepresentation or misleading and deceptive conduct. Under the Australian Consumer Law [17], for example, section 18 prohibits conduct that is misleading or deceptive in trade or commerce. AI systems that generate erroneous outputs, particularly in advisory or decision-support contexts, may expose organisations to liability where reliance

can be established. Furthermore, contractual allocation of risk through disclaimers or limitation clauses may be insufficient where statutory protections apply.

Taken together, these legal challenges demonstrate that AI governance must extend beyond ethical or technical considerations to encompass enforceable legal compliance. The increasing convergence of regulatory frameworks, judicial interpretation, and statutory obligations indicates that organisations must adopt structured legal governance mechanisms to manage liability exposure and ensure compliance. Accordingly, effective AI deployment requires not only technical robustness but also the integration of legal accountability into organisational processes, supported by documentation, auditability, and clear allocation of responsibility.

These legal challenges are not merely theoretical but are increasingly reflected in judicial decisions across multiple jurisdictions. Existing case law provides important doctrinal guidance on how courts approach issues of data protection, liability, and accountability in technology-enabled environments. The following section examines these judicial developments to establish the legal foundations underpinning AI governance.

JUDICIAL APPROACHES TO DATA, LIABILITY AND ALGORITHMIC ACCOUNTABILITY

Building on the legal challenges identified above, this section examines relevant judicial decisions that illustrate how courts have interpreted and applied legal principles to technology-driven contexts. While these cases do not directly address AI systems in all instances, they establish an important doctrinal foundation for understanding legal accountability in AI deployment, particularly as non-compliance may give rise to regulatory sanctions, administrative penalties, and civil liability under emerging regulatory regimes.

The legal challenges arising from the deployment of Artificial Intelligence (AI) systems are increasingly reflected in judicial decisions addressing data protection, digital platform responsibility, and the allocation of liability in technology-enabled environments. While courts have not yet developed a unified body of AI-specific jurisprudence, existing case law provides important doctrinal foundations for understanding legal accountability in AI governance.

Data Protection and Automated Processing

The decision of the Court of Justice of the European Union in Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [14] established that entities engaged in automated data processing may be classified as data controllers and held responsible for ensuring compliance with data protection obligations. The Court emphasised that individuals retain rights over personal data even where processing is carried out through automated indexing and retrieval systems. This principle is directly relevant to AI systems, which similarly rely on large-scale automated processing and raise issues of transparency and accountability.

Subsequent developments in Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [18] reinforced the importance of maintaining robust safeguards where personal data is processed across jurisdictions. The Court's insistence on effective protection of individual rights highlights the regulatory expectation that organisations deploying AI systems must ensure lawful data governance practices irrespective of technological complexity.

Liability and Duty of Care in Technology Contexts

The allocation of liability for AI-generated outcomes may be analysed through established principles of negligence. In Donoghue v Stevenson [15], the House of Lords articulated the foundational duty of care owed by manufacturers to consumers, a principle that may be extended to developers and deployers of AI systems. The application of this principle to AI raises complex questions regarding foreseeability and control, particularly where systems exhibit autonomous or adaptive behaviour.

The refinement of the duty of care test in Caparo Industries plc v Dickman [19] further emphasises the need to establish foreseeability, proximity, and fairness in determining liability. In the context of AI, these elements may be difficult to satisfy where decision-making processes are opaque or distributed across multiple actors, thereby complicating the attribution of legal responsibility.

Misrepresentation and Digital Platform Liability

Courts have also addressed liability arising from misleading information in digital environments. In Hedley Byrne & Co Ltd v Heller & Partners Ltd [20], the House of Lords recognised liability for negligent misstatements where a duty of care exists. This principle is particularly relevant to AI systems that generate recommendations or predictive outputs relied upon in commercial decision-making.

More recently, in Australian Competition and Consumer Commission v Google LLC [21], the High Court of Australia held that Google did not itself engage in misleading conduct through advertisements created by third parties. However, the decision clarified the circumstances under which

digital platforms may bear responsibility for disseminated content. This case illustrates the challenges of assigning liability in complex digital ecosystems and highlights the importance of clearly defining the role of AI systems within commercial transactions.

Algorithmic Decision-Making and Public Law Accountability

The use of algorithmic systems in decision-making has also been scrutinised in public law contexts. In R (Bridges) v Chief Constable of South Wales Police [22], the Court of Appeal found that the use of facial recognition technology was unlawful due to inadequate safeguards and insufficient consideration of privacy rights. The case demonstrates that organisations deploying AI systems must ensure that appropriate governance frameworks are in place to meet legal standards of proportionality, transparency, and accountability.

DISCUSSION

The synthesis of secondary data across empirical studies, governance frameworks, and international standards reveals that effective Artificial Intelligence (AI) governance depends on the organisation's ability to translate ethical principles and regulatory requirements into actionable oversight mechanisms. Three key findings emerged from the integrative analysis: (1) the fragmentation of governance mechanisms across technical, ethical, and legal domains; (2) persistent implementation barriers limiting operationalisation; and (3) the need for integrated frameworks that align AI risk management with strategic decision-making and accountability.

Fragmented and Inconsistent AI Governance Practices

Across the reviewed literature and frameworks, AI governance remains fragmented, with organisations implementing isolated controls, such as bias detection, data security, or compliance checks, without an overarching governance model. Birkstedt et al. [4] identify that most organisations adopt principle-based ethics frameworks that lack operational depth, while Batool et al. [5] note that accountability for AI outcomes is often unclear due to overlapping responsibilities between data scientists, compliance officers, and senior executives.

Similarly, while frameworks such as NIST AI RMF 1.0 [3] and ISO/IEC 42001 [6] provide comprehensive reference points for AI risk and quality management, empirical studies (e.g., Roppelt et al. [7]; Atwal et al. [10]) show that their adoption is uneven across sectors. Many organisations interpret governance narrowly as technical compliance, neglecting cross-functional oversight and ethical assurance processes.

Implications for AI Legal Governance

Collectively, these cases demonstrate that existing legal doctrines, while not developed specifically for AI, provide a robust foundation for addressing the legal challenges associated with automated systems. They underscore the importance of accountability, transparency, and risk allocation in technology deployment. However, they also reveal significant gaps in the current legal framework, particularly in relation to the attribution of liability and the regulation of autonomous decision-making.

These doctrinal developments support the need for structured legal governance frameworks that translate regulatory requirements into operational practices. By embedding legal accountability within organisational processes, such frameworks can mitigate uncertainty and ensure that AI systems operate within clearly defined legal boundaries.

This fragmentation leads to gaps in accountability, insufficient documentation of AI decisions, and inconsistent risk reporting.

The findings underscore that AI governance must move beyond isolated compliance checklists toward integrated systems of control that embed fairness auditing, privacy-by-design, and transparency throughout the AI lifecycle. Governance should be viewed not as an administrative burden but as an enabling mechanism for organisational trust, innovation, and sustainability.

Organisational Barriers to Governance Implementation

Despite the availability of governance models and regulatory guidance, significant barriers continue to impede the practical implementation of responsible AI. These include technological immaturity, data governance deficiencies, organisational resistance, and ethical capacity gaps.

Empirical analyses across sectors demonstrate that legacy IT infrastructure and data silos limit the traceability and explainability of AI decisions [7]. Organisations also face difficulties integrating AI governance into existing corporate risk frameworks, particularly where ethical oversight and technical operations are managed by separate departments. Furthermore, Atwal et al. [10] and the OECD [19] note that the lack of AI literacy among executives hampers effective oversight, resulting in reactive rather than proactive governance.

Cultural resistance also remains a persistent challenge. Governance measures such as algorithmic audits or impact assessments are sometimes perceived as obstacles to innovation or commercial

agility. However, evidence from Wong [9] suggests that embedding ethics-by-design and legal compliance-by-design reduces long-term exposure to liability and reputational harm, creating competitive advantage through responsible innovation.

Addressing these barriers requires not only technical investment but also the establishment of cross-functional governance committees, ethics training, and continuous monitoring mechanisms that reinforce organisational accountability.

Strategic Integration of Governance, Ethics, and Law

The synthesis highlights that effective AI governance requires strategic alignment across the ethical, technical, and legal dimensions of AI use. Organisations that embed governance within corporate strategy, rather than treating it as a compliance exercise, demonstrate stronger resilience, transparency, and stakeholder trust. This strategic integration is also reflected in recent governance guidance from the Australian Institute of Company Directors (AICD) [8], which emphasises the role of boards in overseeing AI-related risks, ensuring accountability, and aligning AI deployment with organisational strategy and risk appetite. The AICD framework highlights that effective AI governance requires not only technical controls but also board-level oversight, clear accountability structures, and ongoing assurance mechanisms. This reinforces the need for governance models that extend beyond operational risk management to encompass corporate governance and legal accountability.

The integration of strategic and legal perspectives is reflected in frameworks such as the EU AI Act [2], which mandates risk classification, documentation, and human oversight for high-risk systems. Similarly, the NIST AI RMF 1.0 [3] emphasises iterative risk mapping and measurement, while ISO/IEC 42001 [6] sets out management system requirements for organisational accountability. Together, these standards define a shared global direction toward measurable, auditable governance.

The reviewed studies indicate that organisations implementing structured governance frameworks experience improved risk visibility, clearer role definitions, and enhanced capacity to meet regulatory expectations. By synthesising these insights, the current study proposes a six-phase AI Legal Governance Framework, which unites the procedural strengths of Roppelt et al. [7], the risk-centric structure of NIST AI RMF 1.0 [3], and the legal-ethical controls articulated by Wong [9].

This integrated model enables organisations to establish governance processes that are strategically aligned, legally compliant, and ethically robust, ensuring that AI deployment contributes to sustainable and trustworthy innovation.

Summary of Findings

In summary, the findings reveal that:

- AI governance remains fragmented and lacks cross-functional integration.
- Implementation is hindered by organisational resistance, data governance limitations, and insufficient ethical capacity.
- Integrated frameworks that align ethical, technical, and legal governance dimensions are essential for sustainable AI adoption.
-

These findings directly inform the development of the proposed six-phase AI Legal Governance Framework, which operationalises responsible AI principles through structured oversight, fairness auditing, privacy-by-design, and compliance assurance.

LEGAL GOVERNANCE FRAMEWORK FOR AI SYSTEMS

The development of a legal governance framework for AI systems is essential for organisations seeking to ensure regulatory compliance, manage legal risk, and maintain accountability in AI deployment.

Frameworks developed by Roppelt et al. [7] and NIST AI RMF 1.0 [3] as well as governance guidance from the Australian Institute of Company Directors (AICD) [8], are further enhanced through the integration of Wong's legal risk governance recommendations [9]. Framework by Roppelt et al. [7]

Roppelt et al. [7] propose a structured four-phase framework for the adoption of Artificial Intelligence (AI), developed within the context of talent management but broadly applicable to organisational AI implementation. The framework adopts a procedural lifecycle approach, progressing from strategic planning to continuous evaluation, and provides a useful foundation for understanding how organisations operationalise AI systems. The framework comprises four key phases:

1. Strategy Development – this involves identifying appropriate use cases for AI deployment and aligning these initiatives with organisational objectives. While originally framed within human resource functions, this phase can be generalised to encompass broader organisational contexts where AI is applied to decision-making processes.
2. Pilot Testing – this emphasises the evaluation of AI systems within controlled environments prior to full-scale deployment. This phase incorporates mechanisms such as fairness auditing, model validation, and iterative refinement to mitigate risks associated with bias, inaccuracy, and unintended outcomes.

3. Full Implementation – this entails the organisation-wide deployment of AI systems, supported by training programs and the establishment of data governance practices. This phase highlights the importance of organisational readiness and the integration of AI into operational workflows.
4. Continuous Review – this focuses on ongoing monitoring and evaluation, including performance assessment, fairness auditing, and feedback mechanisms to ensure that AI systems remain effective and aligned with organisational objectives over time.

While the Roppelt et al. framework provides a robust procedural model for AI adoption, its primary emphasis is on operational implementation rather than legal and regulatory compliance. The framework does not explicitly address issues of legal accountability, liability allocation, or regulatory obligations arising from AI deployment. As such, it highlights a critical gap between procedural AI adoption models and the legal governance requirements identified in contemporary regulatory frameworks.

This limitation reinforces the need for an integrated legal governance approach that embeds compliance, accountability, and risk management within each phase of the AI lifecycle.
Framework aligned to the NIST AI Risk Management Framework (AI RMF 1.0) [3]

The NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) provides a technology and sector agnostic foundation for governing AI across its lifecycle [3]. It organizes governance into four core functions, Map, Measure, Manage, and Govern, that can be operationalised in all organisations:
1. Map – this identifies intended uses, contexts, stakeholders, and risks (including safety, fairness, privacy, security, and environmental impacts).
2. Measure - this develops and applies qualitative and quantitative risk metrics (e.g., bias, drift, robustness, privacy loss) and validates datasets and models.
3. Manage - this prioritises, treats, and monitors risks with controls (e.g., data governance, model cards, human-in-the-loop, incident response) and change management.
4. Govern - this embeds accountability through policies, roles, training, documentation, impact assessments, and continuous improvement.

This risk-centric structure complements prior syntheses of governance mechanisms and provides a practical path from principles to controls.

AICD Governance Guidance [8]

The governance guidance developed by the Australian Institute of Company Directors [8], in collaboration with the Human Technology Institute, provides a board-level approach to AI governance. It focuses on director oversight, accountability, and organisational assurance, and is structured around key elements of effective governance rather than a procedural or risk-based lifecycle.

The AICD guidance identifies core elements that can be operationalised within organisational governance systems:
1. Roles and Responsibilities – this establishes clear accountability for AI decision-making at both board and management levels, including oversight of AI system procurement, deployment, and outcomes.
2. Governance Structures – this determines appropriate board and management structures (e.g., committees, advisory bodies) to support effective oversight of AI-related risks and opportunities.
3. People, Skills and Culture – this emphasises the development of organisational and director-level AI capability, including training, awareness, and the promotion of a governance culture that supports responsible AI use.
4. Principles, Policies and Strategy – this requires the alignment of AI initiatives with organisational strategy, supported by clear policies and ethical principles governing AI deployment across the organisation and its supply chain.
5. Practices, Processes and Controls – this involves implementing governance controls, including risk management frameworks, AI impact assessments, and compliance mechanisms to ensure safe and lawful AI use.
6. Supporting Infrastructure – this focuses on establishing technical and data governance infrastructure, including AI inventories and data management systems, to support transparency and accountability.
7. Stakeholder Engagement and Impact Assessment – this emphasises engagement with stakeholders and the assessment of the societal, ethical, and legal impacts of AI systems, including accessibility and fairness considerations.
8. Monitoring, Reporting and Evaluation – this requires the implementation of continuous monitoring, reporting, and assurance mechanisms, including internal and external audits, to evaluate AI system performance and compliance over time.

The AICD governance guidance highlights that effective AI governance must extend beyond technical risk management to include board-level

oversight, accountability structures, and ongoing assurance. While it does not prescribe detailed operational processes, it provides a critical governance layer that complements procedural and risk-based frameworks. It reinforces the need to integrate AI governance within broader corporate governance systems, ensuring that legal compliance and accountability are embedded at the highest levels of organisational decision-making.

Proposed Governance Framework

While the preceding frameworks provide procedural, risk-based, and governance-oriented perspectives on AI deployment, they do not fully operationalise legal compliance within organisational systems. In particular, they lack an integrated approach that embeds legal accountability, regulatory obligations, and liability management across the AI lifecycle. Consequently, these approaches collectively reveal the absence of a unified legal governance model.

To address this limitation, this study synthesises the procedural approach of Roppelt et al. [7], the risk-based structure of the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) [3], and the governance guidance of the Australian Institute of Company Directors (AICD) [8], with the legal risk governance recommendations advanced by Wong [9]. This integration results in a comprehensive governance framework that aligns operational processes, risk management practices, and corporate oversight with enforceable legal requirements.

Wong [9] identifies several key mechanisms necessary for embedding legal governance in AI systems. These include the use of AI impact assessments to evaluate legal and ethical risks, the implementation of privacy-by-design and robust data governance practices, and the auditing of algorithmic bias to mitigate discrimination risks. The framework further emphasises the need to ensure lawful workplace surveillance practices and to minimise consumer and contractual liability through accurate disclosures and well-structured contractual arrangements.

In addition, the framework incorporates cybersecurity-by-design principles aligned with international standards, ongoing monitoring and auditing of AI systems, and active stakeholder engagement through participatory design processes. Organisations are also required to align proactively with emerging regulatory frameworks, including the EU Artificial Intelligence Act [2] and ISO/IEC standards [6], to ensure forward-looking compliance and regulatory readiness.

This integrated approach directly addresses the fragmentation and operationalisation gaps identified in recent systematic reviews [5], providing a structured and legally grounded model for translating regulatory requirements into organisational practice. It establishes a cohesive governance framework that embeds legal compliance, accountability, and risk management throughout the AI lifecycle, thereby enabling organisations to deploy AI systems in a legally defensible and socially responsible manner.

AI LEGAL GOVERNANCE FRAMEWORK

The integrative synthesis of secondary data culminated in the development of a six-phase AI Legal Governance Framework, designed to translate ethical principles and regulatory requirements into actionable organisational processes. The framework integrates insights from Roppelt et al. [7] on procedural implementation, the NIST AI Risk Management Framework (AI RMF 1.0) [3] on risk governance, and Wong [9] on legal-ethical accountability, while aligning with international standards such as ISO/IEC 42001 [6] and the EU AI Act [2].

This governance model addresses the fragmentation identified in prior studies by uniting the strategic, technical, and legal dimensions of AI oversight into a cohesive system. It enables organisations to operate responsible AI through structured phases of planning, deployment, and continuous assurance. The six phases include:

Phase 1 –Legal and Regulatory Alignment

The first phase establishes the foundation for responsible AI governance by aligning AI initiatives with organisational strategy, ethical values, and legal obligations. It requires senior leadership to define the scope, objectives, and intended outcomes of AI deployment, ensuring they are consistent with corporate strategy and social responsibility commitments. This phase also involves mapping stakeholders, identifying internal and external accountabilities, and defining governance boundaries. Alignment with regulatory instruments such as the EU AI Act [2], OECD AI Principles [1], and NIST AI RMF (Map Function) [3] ensures early recognition of potential ethical and compliance risks.

Phase 2 – Legal Risk Classification and Assessment

Building upon strategic alignment, Phase 2 focuses on the identification and assessment of potential risks, including bias, discrimination, privacy breaches, and model drift. It integrates the "Measure" and "Manage" functions from the NIST AI RMF [3], supported by risk metrics and bias auditing tools. This phase embeds fairness auditing and privacy-by-design methodologies into model development and testing. Risk categories should reflect technical, ethical, and reputational dimensions, ensuring comprehensive evaluation prior to deployment.

Phase 3 – Compliance-by-Design and Legal Controls

Phase 3 operationalises the governance strategy through compliance-by-design, ensuring that accountability, transparency, and compliance mechanisms are embedded into technical and organisational processes from the outset. This involves the establishment of cross-functional oversight structures, such as AI Ethics Committees and Data Governance Boards, to supervise system development and deployment. The phase also aligns with ISO/IEC 42001 principles on documentation [6], version control, and audit trails, ensuring traceability of AI decisions and system modifications.

Phase 4 – Legal and Compliance Capability Development

Effective governance depends on organisational capability. Phase 4 builds internal competence through AI literacy training, ethics workshops, and the development of governance skills across executive, legal, and technical teams. This phase institutionalizes ethical reasoning and compliance awareness, addressing one of the persistent gaps in AI governance identified by Birkstedt et al. (2023) [4]. Training should emphasise accountability roles, explainability principles, and the integration of AI governance into corporate decision-making.

Phase 5 – Continuous Legal Audit and Regulatory Monitoring

Phase 5 ensures that AI governance remains adaptive to changing conditions, regulations, and stakeholder expectations. Continuous monitoring involves periodic fairness audits, incident response reviews, and system recalibration to mitigate model drift and unintended outcomes. This stage aligns with the "Govern" function in the NIST AI RMF [3] and the continuous improvement cycle of ISO/IEC 42001 [6]. Audit mechanisms should be transparent and externally verifiable, enabling organisations to demonstrate compliance and accountability to regulators, customers, and the public.

Phase 6 – Regulatory Compliance and Liability Assurance

The final phase establishes comprehensive legal and regulatory assurance to ensure that AI systems comply with applicable laws and emerging standards. It incorporates AI Impact Assessments (AIAs), algorithmic accountability statements, and cybersecurity-by-design protocols, as recommended by Wong [9]. This phase formalises governance through continuous oversight from cross-functional committees, integrating legal counsel, compliance officers, data scientists, and executives. Organisations are encouraged to align with global frameworks, including the EU AI Act [2], Australia's Privacy Act 1988 [12], and the OECD AI Governance Guidelines [23][24], to maintain global interoperability and trust.

This enhanced framework ensures that AI integration is not only operationally effective but also compliant, transparent, and ethically grounded.

CONCLUSION

Artificial Intelligence (AI) is rapidly reshaping organisational decision-making and commercial practice, but its adoption introduces complex legal and regulatory challenges that extend beyond traditional governance frameworks. This study demonstrates that fragmented approaches to AI oversight, where technical, ethical, and legal considerations are treated in isolation, are insufficient to ensure enforceable accountability, regulatory compliance, and risk mitigation in contemporary AI deployment.

This paper contributes to the field of commercial law and technology by developing a six-phase AI Legal Governance Framework that operationalises regulatory obligations into structured organisational processes. Drawing upon the NIST AI Risk Management Framework, ISO/IEC 42001, and emerging regulatory instruments such as the EU Artificial Intelligence Act, the framework integrates legal alignment, risk classification, compliance-by-design, organisational capability, continuous legal auditing, and regulatory assurance into a cohesive compliance model. In doing so, it bridges the gap between high-level legal principles and practical implementation, enabling organisations to embed compliance within the lifecycle of AI systems.

The framework advances legal scholarship by demonstrating how regulatory requirements, particularly in areas of data protection, algorithmic accountability, and organisational liability, can be translated into enforceable governance mechanisms. It provides a structured approach for addressing key legal risks associated with AI, including bias and discrimination, unlawful data processing, lack of transparency, and liability for automated decision-making. By embedding compliance within organisational systems, the model supports defensible legal positions while reducing exposure to regulatory sanctions and reputational harm.

From a practical perspective, the framework offers organisations a roadmap for transitioning from voluntary ethical guidelines to auditable and legally grounded governance practices. Alignment with international standards and regulatory regimes, including the EU AI Act [2] and Australia's Privacy Act 1988 [12], ensures that organisations can respond proactively to evolving legal expectations while maintaining operational efficiency and stakeholder trust.

This study also contributes to the broader discourse on AI regulation by emphasising that effective governance must be understood as a legal and institutional capability rather than a purely technical or ethical function. It highlights the necessity of integrating legal expertise, compliance structures, and organisational processes to ensure that AI systems operate within clearly defined regulatory boundaries.

Future research should focus on empirically validating the proposed framework across jurisdictions and industry contexts, particularly in relation to its effectiveness in mitigating legal risk and supporting regulatory compliance. Comparative analyses may further examine how differing regulatory regimes influence governance design and organisational accountability.

Ultimately, the governance of AI must be conceived as an ongoing process of legal adaptation, regulatory alignment, and institutional learning. Non-compliance with these frameworks may expose organisations to regulatory sanctions, administrative penalties, and civil liability, reinforcing the need for structured legal governance. The framework presented in this study provides a foundation for that process, transforming AI governance from a conceptual aspiration into a structured, operational, and legally defensible model suitable for contemporary commercial environments.

REFERENCES

1. Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence, Paris, France: OECD, 2019.
2. European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Brussels, Belgium: Official Journal of the European Union, June 2024.
3. National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, Jan. 2023, doi: 10.6028/NIST.AI.100-1.
4. Birkstedt T, Minkkinen M, Tandon A, Mäntymäki M. "AI governance: Themes, knowledge gaps and future agendas." Internet Research, vol. 33, no. 7, pp. 133–167, 2023. doi: 10.1108/INTR-01-2022-0042.
5. Batool A, Zowghi D, Bano M. "AI governance: A systematic literature review." AI and Ethics, 2024. doi: 10.1007/s43681-024-00653-w.
6. International Organisation for Standardization, ISO/IEC 42001:2023 – Artificial Intelligence Management System (AIMS) — Requirements. Geneva, Switzerland: ISO, 2023.
7. Roppelt JS, Greimel NS, Kanbach DK, Stubner S, Maran TK. "Artificial intelligence in talent acquisition: A multiple case study on multi-national corporations." Management Decision, vol. 62, no. 10, pp. 2986–3007, 2024. doi: 10.1108/MD-07-2023-1194.
8. Australian Institute of Company Directors, A Director's Guide to AI Governance, Sydney, Australia: AICD, 2024. Available: https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-resources/a-directors-guide-to-ai-governance-web.pdf
9. Wong B. "AI in corporations: Legal and environmental risks and their impact on leadership, governance, and sustainability in Australia." International Journal of Environmental Sciences, vol. 11, no. 20s, pp. 467–474, 2025. Available: https://theaspd.com/index.php/ijes/article/view/5751/4167
10. Atwal GF, Bryson D, Williams A. "An exploratory study of the adoption of artificial intelligence in Burgundy's wine industry." Strategic Change, vol. 30, no. 3, pp. 299–306, 2021. doi: 10.1002/jsc.2413.
11. Jhansi Rani MR, Vishnu Priya LV, Venkata Krishna Prasad CB. "AI in HR: Revolutionizing recruitment, retention, and employee engagement." Journal of Informatics Education and Research, vol. 4, no. 3, 2024. doi: 10.52783/jier.v4i3.1410.
12. Australian Government, Privacy Act 1988 (Cth), Canberra, ACT: Federal Register of Legislation, 2023 (reprint).
13. European Parliament and Council of the European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Official Journal of the European Union, L119, 4 May 2016.
14. Google Spain SL v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, CJEU, 13 May 2014.
15. Donoghue v Stevenson [1932] AC 562 (HL).
16. Lloyd v Google LLC [2021] UKSC 50.
17. Competition and Consumer Act 2010 (Cth), Sch 2 (Australian Consumer Law), s 18.

18. Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems (Schrems II), Case C-311/18, EU:C:2020:559, CJEU, 16 July 2020.
19. Caparo Industries plc v Dickman [1990] 2 AC 605 (HL).
20. Hedley Byrne & Co Ltd v Heller & Partners Ltd [1964] AC 465 (HL).
21. Australian Competition and Consumer Commission v Google LLC [2021] HCA 27.
22. R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.
23. OECD, OECD Framework for the Classification of AI Systems, Paris, France: OECD Digital Economy Policy Committee, 2022.
24. OECD, "AI, Data Governance and Privacy: Synergies and Areas of International Co-operation." OECD Artificial Intelligence Papers No. 22, 26 Jun. 2024. doi: 10.1787/2476b1a4-en.

