

Human-Centred Governance for Responsible AI Adoption: Enabling Sustainable Business Transformation and Societal Value

Bernard Wong^{1,2}

¹Enterprise Strategy Consulting Inc, Sydney, NSW 2073, Australia

²Wentworth Institute of Higher Education, Sydney, NSW 2010, Australia

ABSTRACT

Artificial Intelligence (AI) is transforming organisational operations and strategic decision-making, but its rapid adoption has outpaced the development of governance mechanisms capable of supporting sustainable growth and societal outcomes. Organisations face increasing challenges in translating ethical principles and regulatory requirements into actionable governance processes that align with business strategy and stakeholder expectations. This study develops a six-phase human-centred governance framework for responsible AI adoption through an integrative synthesis of academic literature, international standards, and regulatory frameworks, including the NIST AI Risk Management Framework, ISO/IEC 42001, and the European Union Artificial Intelligence Act. The proposed framework integrates strategic alignment, risk management, governance-by-design, organisational capability, continuous monitoring, and legal assurance into a structured and repeatable model. By positioning AI governance as a strategic capability rather than a compliance function, the framework provides a practical roadmap for organisations to embed responsible AI practices that enhance transparency, accountability, and trust. The study contributes to the field of human factors in business management by demonstrating how governance can enable sustainable organisational performance while supporting broader societal impact.

Keywords: Artificial intelligence governance, Sustainable business, Societal value, Digital transformation, Human factors, Organisational governance

INTRODUCTION

Artificial Intelligence (AI) is transforming organisational operations, business models, and strategic decision-making across industries, playing a central role in digital transformation within the Fourth Industrial Revolution. While AI offers significant opportunities for innovation and competitive advantage, its rapid adoption has outpaced the development of governance mechanisms capable of supporting sustainable growth and societal outcomes. As AI systems are increasingly embedded in critical domains such as finance, healthcare, public services, and human resources, organisations face growing

challenges related to accountability, transparency, fairness, and regulatory compliance. These challenges extend beyond technical risk to encompass legal, ethical, and societal implications that directly affect stakeholder trust and organisational legitimacy.

From a business and human factors perspective, AI adoption is not solely a technical issue but a strategic and organisational challenge requiring the integration of governance, leadership, and culture. Organisations must balance economic performance with ethical responsibility and social considerations, yet many struggle to embed responsible AI practices within their operational and strategic frameworks. This often results in fragmented governance approaches that fail to address the broader organisational and societal impact of AI-driven transformation.

Artificial Intelligence (AI) governance also introduces significant human factors challenges that extend beyond technical and regulatory considerations. Organisations must address issues such as cognitive load in AI-assisted decision-making, trust in automated systems, human–AI interaction, and the allocation of accountability between humans and intelligent systems. Poorly governed AI can lead to automation bias, reduced situational awareness, and over-reliance on algorithmic outputs, undermining both decision quality and organisational performance. Effective governance therefore requires the integration of human factors principles that support transparency, interpretability, and meaningful human oversight.

Despite the emergence of ethical guidelines and regulatory frameworks, including the OECD AI Principles (OECD, 2019), the European Union Artificial Intelligence Act (European Union, 2024), and the NIST AI Risk Management Framework (NIST, 2023), translating these high-level principles into actionable governance processes remains a persistent challenge. Existing approaches often emphasise compliance or technical risk management in isolation, without integrating strategic, ethical, and legal considerations into organisational decision-making. As a result, organisations continue to face difficulties operationalising responsible AI in ways that align with business objectives and stakeholder expectations.

Prior research has begun to explore both the opportunities and challenges associated with AI adoption in organisational contexts. Earlier work on AI-driven talent management, presented in academic and professional forums, examined the application of AI within human resource functions, highlighting its capacity to enhance recruitment efficiency, workforce planning, and data-driven decision-making. While this work demonstrated significant operational benefits, it also identified emerging concerns related to algorithmic bias, data privacy, and regulatory compliance, indicating that the adoption of AI introduces risks that extend beyond functional performance.

Building on these insights, earlier research (Wong, 2025) examined the legal and governance implications of AI in corporate environments. The study identified key risks, including data privacy breaches, algorithmic discrimination, workplace surveillance, and cybersecurity vulnerabilities, and demonstrated that these risks constitute systemic legal and organisational challenges rather than isolated technical issues. It further established that

responsible AI governance is essential for legal compliance, ethical conduct, and sustainable corporate practice.

Extending this work, subsequent research (Wong, 2026, under review) develops a six-phase AI legal governance framework that operationalises legal and regulatory requirements within organisational processes. The framework integrates obligations arising from data protection law, the EU Artificial Intelligence Act, and international standards into structured phases of governance, including legal alignment, risk classification, compliance-by-design, and continuous audit. This provides organisations with a practical mechanism to manage legal risk, ensure regulatory compliance, and strengthen accountability in AI deployment.

While the six-phase AI legal governance framework provides a structured approach to embedding regulatory compliance, accountability, and legal risk management within organisational processes, its primary focus is on legal and regulatory dimensions of governance. It does not fully address how governance mechanisms are embedded within organisational systems, human decision-making processes, and socio-technical environments. This highlights the need to extend legal governance models by incorporating human factors, organisational capability, and strategic alignment to support effective implementation in practice.

Recent studies (e.g., Birkstedt et al., 2023; Batool et al., 2024) further highlight persistent gaps, including the absence of unified governance frameworks, limited evidence of implementation effectiveness, and insufficient cross-functional accountability. These challenges are compounded by organisational barriers such as limited AI literacy, cultural resistance, and the complexity of integrating governance into existing business processes.

This paper addresses these gaps by extending prior work on AI legal governance to propose a six-phase human-centred governance framework for responsible AI adoption. Drawing on international standards and empirical research, including the NIST AI Risk Management Framework (NIST, 2023), ISO/IEC 42001 (ISO, 2023), and the EU AI Act (European Union, 2024), the framework integrates strategic, organisational, and human factors dimensions of governance. It builds on the legal and procedural foundations established in prior research to operationalise key principles such as fairness, accountability, and cross-functional oversight within organisational and socio-technical contexts.

By positioning AI governance as a socio-technical and strategic organisational capability, rather than solely a compliance function, this study contributes to human factors in business management. The framework supports organisations in aligning AI initiatives with business strategy, regulatory expectations, and societal needs, thereby enhancing organisational performance and enabling sustainable value creation.

INTEGRATIVE ANALYTICAL APPROACH

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) adoption and governance.

Rather than generating new empirical data, the study consolidates insights from multiple authoritative sources to develop a human-centred governance framework that integrates strategic, ethical, and legal dimensions. This approach aligns with established literature synthesis methods that combine conceptual mapping and cross-framework comparison to address fragmentation in AI governance research (Birkstedt et al., 2023; Batool et al., 2024).

Scope of Data Sources

The analysis draws on three categories of sources. First, peer-reviewed empirical studies examining AI adoption across organisational contexts, including Roppelt et al. (2024) on talent acquisition, Atwal et al. (2021) on strategic adoption, and Jhansi Rani et al. (2024) on AI in human resource management. Second, international governance frameworks and standards, including the NIST AI Risk Management Framework (NIST, 2023), ISO/IEC 42001 (ISO, 2023), and the European Union Artificial Intelligence Act (European Union, 2024), which provide global benchmarks for risk-based AI governance. Third, conceptual and review studies, such as Birkstedt et al. (2023) and Wong (2025), which identify ethical, legal, and organisational gaps in current practices.

These sources were selected based on their academic credibility, relevance to AI governance, and recency, ensuring alignment with current developments in responsible AI and organisational governance.

Analytical Process

The synthesis followed a three-stage process. First, key governance mechanisms were identified through structured review, including accountability structures, auditing practices, risk controls, and ethical design principles. Second, these mechanisms were compared across studies and frameworks to identify areas of convergence and divergence between technical, ethical, and regulatory perspectives. Third, the findings were integrated to develop a six-phase governance framework that combines procedural implementation models (Roppelt et al., 2024), risk-based controls (NIST, 2023), and legal-ethical governance principles (Wong, 2025).

Rationale for the Integrative Approach

An integrative synthesis is appropriate for this study as AI governance spans multiple domains, including technology, law, ethics, and organisational management. By consolidating insights across these domains, the study addresses the fragmentation identified in prior research and provides a structured, practical framework for responsible AI adoption. This approach supports the development of governance models that are both theoretically grounded and applicable in organisational contexts.

FINDINGS AND DISCUSSION

The integrative synthesis indicates that effective Artificial Intelligence (AI) governance depends on an organisation's ability to translate ethical principles and regulatory requirements into structured, actionable processes. Three key findings emerge: (1) fragmentation across governance domains, (2) organisational barriers to implementation, and (3) the need for integrated governance aligned with business strategy and accountability.

Fragmented and Inconsistent AI Governance Practices

AI governance remains fragmented across organisations, with many implementing isolated controls—such as bias detection, data security, or compliance checks—without an overarching governance model. Prior studies highlight that principle-based frameworks often lack operational depth, while accountability is frequently unclear due to overlapping responsibilities between technical, legal, and managerial roles (Birkstedt et al., 2023; Batool et al., 2024).

Although frameworks such as the NIST AI Risk Management Framework (NIST, 2023) and ISO/IEC 42001 (ISO, 2023) provide comprehensive guidance, their adoption is uneven. Empirical studies (Roppelt et al., 2024; Atwal et al., 2021) show that organisations often interpret governance narrowly as technical compliance, neglecting cross-functional oversight and ethical assurance. This results in gaps in accountability, limited transparency, and inconsistent risk reporting.

These findings suggest that AI governance must move beyond isolated controls toward integrated systems that embed fairness, transparency, and accountability throughout the AI lifecycle. Rather than acting as a compliance burden, governance should support trust, innovation, and sustainable organisational performance.

Organisational Barriers to Governance Implementation

Despite the availability of governance frameworks, organisations face persistent barriers in operationalising responsible AI. These include technological limitations, data governance challenges, organisational resistance, and insufficient AI literacy.

Legacy systems and data silos limit traceability and explainability of AI outputs, while governance responsibilities are often fragmented across departments. Additionally, limited executive understanding of AI risks contributes to reactive rather than proactive governance approaches (Atwal et al., 2021; OECD, 2024).

Cultural resistance further complicates implementation, as governance measures may be perceived as constraints on innovation. However, embedding ethics-by-design and compliance-by-design can reduce long-term legal and reputational risks while supporting sustainable value creation (Wong, 2025).

Leadership capability is critical in addressing these challenges. Effective governance requires clear accountability structures, informed decision-making, and the integration of governance into organisational culture.

Leaders must develop sufficient AI literacy to evaluate risks and align AI initiatives with strategic objectives, reinforcing governance as a core management responsibility.

Strategic Integration of Governance, Ethics, and Law

The analysis highlights the importance of integrating governance within organisational strategy rather than treating it as a standalone compliance function. Organisations that align governance with strategic objectives demonstrate stronger resilience, improved transparency, and higher levels of stakeholder trust.

This integration is reflected in regulatory and standards frameworks such as the EU AI Act (European Union, 2024), which mandates risk classification and oversight, the NIST AI RMF (NIST, 2023), which emphasises continuous risk management, and ISO/IEC 42001 (ISO, 2023), which establishes organisational accountability structures. Together, these frameworks provide a foundation for governance systems that are measurable, auditable, and aligned with business objectives.

Building on these insights, this study proposes a six-phase governance framework that integrates procedural implementation (Roppelt et al., 2024), risk-based controls (NIST, 2023), and legal-ethical principles (Wong, 2025). This integrated approach supports organisations in aligning governance with both operational and strategic priorities.

AI Governance as a Driver of Sustainable Business and Societal Outcomes

The findings indicate that effective AI governance can act as a driver of both organisational performance and broader societal outcomes. Organisations that implement structured governance frameworks benefit from improved decision-making, enhanced transparency, and increased stakeholder trust.

This dual role reflects the concept of shared value, where organisational success is achieved through the simultaneous creation of economic and societal benefits (Porter and Kramer, 2011). In this context, governance enables organisations to align AI adoption with both business objectives and societal expectations.

By embedding governance within organisational strategy and culture, AI systems can support sustainable innovation, enhance organisational resilience, and contribute to long-term value creation across business and societal contexts.

Summary of Findings

The findings highlight three key conclusions. First, AI governance remains fragmented and lacks integration across technical, ethical, and organisational domains. Second, implementation is constrained by organisational and cultural barriers, including limited AI literacy and governance capability. Third, integrated governance frameworks that align strategy, risk management, and accountability are essential for responsible AI adoption.

These insights inform the development of the proposed six-phase governance framework, which provides a structured approach to embedding responsible AI within organisational systems.

THE STRATEGIC FRAMEWORK FOR AI ADOPTION

A strategic framework for AI adoption is essential for organisations seeking to drive digital transformation and create sustainable value. Existing approaches, including Roppelt et al. (2024) and the NIST AI Risk Management Framework (NIST, 2023), provide complementary foundations that can be integrated with legal and ethical governance principles (Wong, 2025) to support responsible AI implementation.

Framework by Roppelt et al. (2024)

Roppelt et al. (2024) propose a four-phase model comprising strategy development, pilot testing, implementation, and continuous review. The framework emphasises aligning AI initiatives with organisational objectives, testing systems in controlled environments, and refining them through ongoing evaluation. While originally applied to talent management, the model provides a structured basis for broader organisational adoption.

NIST AI Risk Management Framework (NIST, 2023)

The NIST framework organises AI governance into four functions: Map, Measure, Manage, and Govern. These support the identification of risks, evaluation of system performance, implementation of controls, and establishment of accountability structures. This risk-based approach provides a practical foundation for embedding governance within organisational processes.

Toward an Integrated Governance Approach

While these frameworks provide valuable guidance, they do not fully address the organisational and legal complexity of AI adoption. Integrating these models with legal and ethical governance principles (Wong, 2025) enables a more comprehensive approach that incorporates accountability, transparency, and stakeholder considerations. This integration forms the basis of the six-phase governance framework proposed in this study.

GOVERNANCE FRAMEWORK FOR RESPONSIBLE AI ADOPTION

The proposed framework builds upon prior work on AI legal governance by extending the focus from regulatory compliance to organisational and human-centred implementation. While earlier frameworks emphasise legal alignment, risk classification, and compliance assurance, the present model incorporates human factors, organisational capability, and strategic integration as core components of governance. This shift reflects the recognition that effective AI governance requires not only compliance with legal obligations but also the

embedding of governance practices within organisational culture, decision-making processes, and socio-technical systems.

The integrative synthesis of secondary data culminates in the development of a six-phase **human-centred governance framework for responsible AI adoption**, designed to translate ethical principles and regulatory requirements into actionable organisational practices that support sustainable value creation across organisational and societal contexts. The framework integrates procedural insights from Roppelt et al. (2024), risk-based governance from the NIST Artificial Intelligence Risk Management Framework (NIST, 2023), and legal-ethical accountability principles from Wong (2025). It further extends subsequent operational governance work (Wong, 2026, under review) into organisational and human-centred contexts, while aligning with international standards such as ISO/IEC 42001 (ISO, 2023) and the European Union Artificial Intelligence Act (European Union, 2024).

This governance model addresses the fragmentation identified in prior research by uniting strategic, technical, organisational, and legal dimensions of AI oversight into a cohesive socio-technical system. It enables organisations to operationalise responsible AI in a manner that aligns business objectives with ethical responsibility, regulatory compliance, and stakeholder expectations. Importantly, the framework positions governance not only as a risk management function but as a strategic enabler of sustainable growth, organisational resilience, and long-term shared value.

The six phases of the framework are outlined below.

Phase 1 – Strategic Alignment and Context Definition

The first phase establishes the foundation for responsible AI governance by aligning AI initiatives with organisational strategy, sustainability objectives, and societal expectations. Senior leadership defines the scope, purpose, and intended outcomes of AI adoption, ensuring that initiatives contribute to both business performance and broader stakeholder value.

This phase includes the identification of key stakeholders, the mapping of organisational and societal accountabilities, and the definition of governance boundaries. Alignment with regulatory instruments such as the EU AI Act (European Union, 2024), OECD AI Principles (OECD, 2019), and the NIST AI RMF (Map function) (NIST, 2023) supports early recognition of ethical, legal, and social risks. By embedding sustainability and shared value considerations at the outset, organisations can ensure that AI adoption is aligned with long-term organisational goals and societal impact. This phase extends beyond legal alignment by emphasising stakeholder expectations, organisational context, and societal value as key drivers of governance design.

Phase 2 – Risk Mapping and Bias Mitigation

Building upon strategic alignment, Phase 2 focuses on identifying and assessing a comprehensive range of risks associated with AI deployment, including technical, ethical, legal, and societal risks. These include bias, discrimination,

privacy breaches, model drift, and potential impacts on stakeholder trust and social equity.

This phase integrates the “Measure” and “Manage” functions of the NIST AI RMF (NIST, 2023), supported by risk metrics, impact assessments, and bias auditing tools. It embeds fairness auditing, privacy-by-design, and responsible data governance into model development and testing. By extending risk assessment beyond technical performance to include reputational and societal dimensions, organisations can better manage the broader implications of AI adoption and support sustainable and responsible innovation. In contrast to purely compliance-driven approaches, this phase incorporates human and societal risk dimensions, including trust, fairness perception, and stakeholder impact.

Phase 3 – Governance-by-Design and Implementation Control

Phase 3 operationalises governance through a governance-by-design approach, ensuring that accountability, transparency, and ethical considerations are embedded into both technical systems and organisational processes from the outset. This approach integrates human factors principles into system design, supporting interpretability, human oversight, and responsible decision-making.

Key activities include the establishment of cross-functional governance structures, such as AI Ethics Committees and Data Governance Boards, which provide oversight across organisational functions. These structures facilitate coordination between technical, legal, and business teams, ensuring that AI deployment aligns with organisational strategy and stakeholder expectations. Alignment with ISO/IEC 42001 (ISO, 2023) further supports documentation, traceability, and auditability of AI systems, enhancing organisational transparency and trust. This phase emphasises human-centred design principles, including interpretability, usability, and meaningful human oversight, to support effective human–AI interaction.

Phase 4 – Capacity Building and Organisational Competence

Effective governance requires strong organisational capability. Phase 4 focuses on developing human capital, organisational culture, and governance competence to support responsible AI adoption. This includes AI literacy training, ethics education, and the development of governance skills across leadership, legal, and technical functions.

From a human factors perspective, this phase addresses the cognitive and organisational challenges associated with AI adoption, including decision-making complexity, accountability, and trust in automated systems. By embedding governance awareness within organisational culture, organisations can foster responsible innovation, strengthen collaboration, and support sustainable transformation.

This phase also contributes to long-term value creation by enhancing workforce capability and aligning organisational practices with ethical and societal expectations. This reflects the critical role of organisational culture,

leadership capability, and AI literacy in enabling governance to be embedded effectively within practice.

Phase 5 – Continuous Monitoring, Audit, and Improvement

Phase 5 ensures that AI governance remains dynamic and responsive to evolving business conditions, regulatory requirements, and societal expectations. Continuous monitoring involves regular fairness audits, performance evaluations, and incident reviews to identify and mitigate emerging risks.

This phase aligns with the “Govern” function of the NIST AI RMF (NIST, 2023) and the continuous improvement cycle of ISO/IEC 42001 (ISO, 2023), emphasising transparency, accountability, and adaptability. Importantly, monitoring extends beyond technical performance to include organisational outcomes, stakeholder trust, and societal impact.

By incorporating feedback mechanisms and performance metrics, organisations can continuously refine AI systems and governance processes, ensuring alignment with both strategic objectives and sustainable development goals.

Phase 6 – Legal Compliance and Assurance

The final phase establishes comprehensive legal and regulatory assurance, ensuring that AI systems comply with applicable laws and emerging global standards. This includes the implementation of AI Impact Assessments (AIAs), algorithmic accountability frameworks, and cybersecurity-by-design practices, as recommended by Wong (2025).

This phase formalises governance through structured oversight involving legal counsel, compliance officers, data scientists, and executive leadership. Organisations are encouraged to align with global frameworks, including the EU AI Act (European Union, 2024), Australia’s Privacy Act 1988 (Australian Government, 2023), and OECD AI governance guidelines (OECD, 2022; OECD, 2024), to ensure interoperability, regulatory compliance, and trust across jurisdictions.

Beyond compliance, this phase reinforces the organisation’s commitment to ethical responsibility and societal value, ensuring that AI adoption contributes to long-term sustainability, stakeholder confidence, and responsible business practice. While legal compliance remains essential, this phase situates regulatory assurance within a broader organisational and governance context that supports sustainable and responsible AI adoption.

This enhanced framework ensures that AI adoption is not only operationally effective but also strategically aligned, ethically grounded, and socially responsible. By integrating governance into organisational strategy and culture, the framework enables organisations to balance economic performance with ethical accountability and societal impact.

As such, the framework positions AI governance as a key enabler of sustainable business transformation, supporting innovation, competitive advantage, and long-term shared value in an increasingly complex digital environment.

CONCLUSION

Artificial Intelligence (AI) is reshaping organisational decision-making and business processes, but its rapid adoption has outpaced the development of governance mechanisms capable of supporting sustainable and responsible use. This study demonstrates that fragmented approaches to AI governance are insufficient, highlighting the need for integrated frameworks that align technical, ethical, and organisational considerations. This study extends prior legal governance frameworks by demonstrating how AI governance can be embedded within organisational systems, human decision-making processes, and strategic management practices.

The six-phase human-centred governance framework developed in this study provides a structured approach to operationalising responsible AI. By integrating strategic alignment, risk management, governance-by-design, organisational capability, continuous monitoring, and legal assurance, the framework enables organisations to embed governance within their operations and decision-making processes.

From a business and societal perspective, the framework positions AI governance as a strategic capability that supports transparency, accountability, and stakeholder trust. In doing so, it enables organisations to align AI adoption with both business objectives and broader societal outcomes.

While the framework offers a practical contribution, future research should focus on empirical validation across different organisational contexts and industries. Such research would further assess its effectiveness in supporting governance maturity, organisational performance, and stakeholder trust.

Ultimately, AI governance should be understood as an ongoing organisational capability rather than a static compliance requirement. The framework presented in this study provides a foundation for managing the complexity of AI-driven transformation and supporting sustainable value creation.

REFERENCES

- Atwal, G.F., Bryson, D. and Williams, A. (2021) 'An exploratory study of the adoption of artificial intelligence in Burgundy's wine industry', *Strategic Change*, 30(3), pp. 299–306. <https://doi.org/10.1002/jsc.2413>
- Australian Government (2023) *Privacy Act 1988 (Cth)*. Canberra: Federal Register of Legislation.
- Batool, A., Zowghi, D. and Bano, M. (2024) 'AI governance: A systematic literature review', *AI and Ethics*. <https://doi.org/10.1007/s43681-024-00653-w>
- Birkstedt, T., Minkkinen, M., Tandon, A. and Mäntymäki, M. (2023) 'AI governance: Themes, knowledge gaps and future agendas', *Internet Research*, 33(7), pp. 133–167. <https://doi.org/10.1108/INTR-01-2022-0042>
- European Union (2024) *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Brussels: Official Journal of the European Union.
- International Organization for Standardization (ISO) (2023) *ISO/IEC 42001:2023 – Artificial Intelligence management system (AIMS) — Requirements*. Geneva: ISO.

- Jhansi Rani, M.R., Vishnu Priya, L.V. and Venkata Krishna Prasad, C.B. (2024) 'AI in HR: Revolutionizing recruitment, retention, and employee engagement', *Journal of Informatics Education and Research*, 4(3). <https://doi.org/10.52783/jier.v4i3.1410>
- NIST (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. <https://doi.org/10.6028/NIST.AI.100-1>
- OECD (2019) *OECD Principles on Artificial Intelligence*. Paris: Organisation for Economic Co-operation and Development.
- OECD (2022) *OECD Framework for the Classification of AI Systems*. Paris: OECD Digital Economy Policy Committee.
- OECD (2024) *AI, data governance and privacy: Synergies and areas of international co-operation*. OECD Artificial Intelligence Papers No. 22. <https://doi.org/10.1787/2476b1a4-en>
- Porter, M.E. and Kramer, M.R. (2011) 'Creating shared value', *Harvard Business Review*, 89(1–2), pp. 62–77.
- Roppelt, J.S., Greimel, N.S., Kanbach, D.K., Stubner, S. and Maran, T.K. (2024) 'Artificial intelligence in talent acquisition: A multiple case study on multinational corporations', *Management Decision*, 62(10), pp. 2986–3007. <https://doi.org/10.1108/MD-07-2023-1194>
- Wong, B. (2025) 'AI in corporations: Legal and environmental risks and their impact on leadership, governance, and sustainability in Australia', *International Journal of Environmental Sciences*, 11(20s), pp. 467–474. Available: <https://theaspd.com/index.php/ijes/article/view/5751/4167>
- Wong, B. (2026) "Operationalising AI Legal Governance: A Regulatory Compliance Framework for AI Systems". *Journal of International Commercial Law and Technology* 7(1), pp 1374–1384. Available: <https://jiclt.com/article/operationalising-AI-legal-governance-a-regulatory-compliance-framework-for-ai-systems--459/>