Measuring AI Governance: A Capability Maturity Model for Board-Level Oversight

Professor Bernard Wong [1 2]

[1] Enterprise Strategy Consulting Inc, Australia

[2] Wentworth Institute of Higher Education, Australia

DOI: https://doi.org/10.51244/IJRSI.2026.1306000122

Received: 07 June 2026; Accepted: 12 June 2026; Published: 25 June 2026

ABSTRACT

Artificial Intelligence (AI) governance has emerged as a critical organisational and board-level concern as AI systems become increasingly embedded in business operations and decision-making. Although existing AI maturity models assess technological capability and deployment readiness, they provide limited mechanisms for evaluating governance effectiveness, accountability, and board oversight. Consequently, organisations lack structured approaches for assessing whether AI governance practices are achieving their intended objectives.

This study addresses this gap through the development of an AI Governance Capability Maturity Model that reconceptualises AI governance as a measurable organisational capability. Using a qualitative integrative synthesis of regulatory frameworks, legal doctrine, governance standards, and academic literature, the study identifies key governance mechanisms and integrates them within a six-phase governance framework. These governance phases are subsequently transformed into a five-level maturity model supported by a multi-dimensional measurement architecture comprising input, process, output, and outcome metrics.

The analysis demonstrates that existing maturity models focus primarily on AI deployment capability, while governance-oriented frameworks emphasise operational controls but provide limited support for performance evaluation, strategic governance, and board-level accountability. To address these limitations, the proposed model links governance processes to measurable indicators and maturity levels, enabling organisations to assess governance effectiveness, identify capability gaps, and monitor continuous improvement.

The study contributes to theory by positioning AI governance as a dynamic organisational capability rather than a collection of compliance activities. It contributes to practice by providing a structured framework that supports governance assessment, performance monitoring, and board oversight. The model aligns with emerging governance expectations reflected in the NIST AI Risk Management Framework, ISO/IEC 42001, and the European Union Artificial Intelligence Act.

By integrating governance processes, capability development, maturity assessment, and performance measurement, the proposed framework provides a practical and theoretically grounded approach for advancing responsible AI adoption and strengthening board-level governance oversight.

Keywords: Artificial Intelligence Governance, Governance Capability Maturity Model, Board-Level Oversight, Responsible AI, AI Risk Management

INTRODUCTION

Artificial Intelligence (AI) is increasingly embedded in organisational operations, decision-making processes, and strategic functions, creating both significant opportunities and complex governance challenges. As AI systems are deployed across critical domains such as finance, healthcare, human resources, and public administration, organisations face growing pressures to ensure accountability, transparency, fairness, and compliance with evolving legal and regulatory requirements. These challenges extend beyond technical risk management to encompass broader legal, ethical, and organisational considerations that directly affect stakeholder trust and corporate legitimacy (Floridi et al., 2018; Jobin, Ienca and Vayena, 2019; Mittelstadt,

2019).

In response, a growing body of research has emphasised the importance of structured AI governance frameworks. Prior studies demonstrate that AI-related risks, including data privacy breaches, algorithmic discrimination, and liability arising from automated decision-making, are not isolated technical issues but systemic governance concerns requiring coordinated organisational and legal responses (Raji et al., 2020; OECD, 2019). Frameworks such as the National Institute of Standards and Technology AI Risk Management Framework (National Institute of Standards and Technology (NIST), 2023) and ISO/IEC 42001 (ISO, 2023) provide important guidance for managing these risks.

However, a critical limitation remains. Existing frameworks primarily define what organisations should do but provide limited guidance on how governance effectiveness can be evaluated (Wendler, 2012; Sonntag et al., 2024). As a result, organisations lack structured mechanisms for assessing governance performance, monitoring risk exposure, and ensuring continuous improvement.

This limitation is particularly significant at the level of corporate governance. Boards of directors are increasingly responsible for overseeing AI-related risks and ensuring compliance with legal and regulatory obligations (Tricker, 2019; Mallin, 2019). Yet, without measurable indicators of governance capability, boards are unable to determine whether governance mechanisms are functioning effectively or to exercise meaningful oversight.

This paper addresses this gap by advancing AI governance from a procedural framework to a measurable organisational capability. Building on prior work that developed a six-phase AI governance framework (Wong, 2025; Wong, 2026), the study introduces a governance capability maturity model that enables organisations to assess, monitor, and improve governance effectiveness. The model integrates six capability domains, regulatory intelligence, risk assessment, governance-by-design, organisational capability, continuous assurance, and external accountability, within a five-level maturity structure.

By linking governance processes to measurable outcomes and board-level oversight, the study provides a structured mechanism for evaluating governance performance. This perspective aligns with capability-based theory, which emphasises the importance of organisational ability to integrate and continuously improve complex processes in dynamic environments (Teece, 2007; Eisenhardt and Martin, 2000). In doing so, the study contributes to the fields of corporate governance, information systems, and technology law by bridging the gap between governance design and governance performance, and by positioning AI governance as a strategic organisational capability rather than a purely compliance-driven function.

LITERATURE REVIEW

Deployment-Focused AI Maturity Models

Maturity models have long been employed as structured mechanisms for assessing organisational capability, guiding digital transformation, and supporting continuous improvement. Originating in software engineering (e.g., Capability Maturity Model Integration), these models have been widely adapted to evaluate emerging technologies, including Artificial Intelligence (AI) (Wendler, 2012; Schumacher, Erol and Sihn, 2016). In the AI context, maturity models predominantly focus on deployment capability, defined as an organisation's ability to adopt, implement, scale, and operationalise AI systems (Dwivedi, Y.K. et al., 2021).

A comprehensive synthesis of this literature is provided by Sonntag et al. (2024), who analyses 81 academic and industry publications and identify eleven prominent AI maturity models. These models, developed across consulting, industry, and academic domains, assess organisational progression from experimental AI adoption to enterprise-wide integration.

The identified models, including those developed by Gartner, McKinsey & Company, Accenture, Deloitte, IBM, Microsoft, PwC, Boston Consulting Group, and others, exhibit strong structural convergence. Most define four to six maturity levels, progressing from ad hoc experimentation to optimised, enterprise-wide AI deployment.

They also assess maturity across common capability dimensions, including strategy, data infrastructure, technology platforms, organisational structure, talent, and development processes (Sonntag et al., 2024).

These models make several important contributions. They provide structured mechanisms for assessing AI adoption, enable benchmarking across organisations, and offer roadmaps for capability development. In particular, they translate the abstract concept of "AI readiness" into measurable organisational constructs, supporting strategic planning and investment decisions (Wendler, 2012).

However, despite their methodological sophistication, these models exhibit a consistent limitation: they primarily evaluate technical and operational capability, rather than governance effectiveness (Sonntag et al., 2024).

Governance-Oriented AI Maturity Models

As concerns regarding the ethical, legal, and societal implications of artificial intelligence have intensified, a second stream of maturity models has emerged that places greater emphasis on governance considerations. Unlike deployment-focused models, which primarily assess technological capability and organisational readiness, governance-oriented frameworks seek to address issues relating to accountability, transparency, risk management, compliance, and responsible AI practices.

A prominent example is the OWASP AI Maturity Assessment (AIMA), which extends maturity assessment beyond technical implementation to encompass governance, privacy, security, ethical considerations, and lifecycle management. The framework adopts a multi-domain approach that evaluates governance activities across the AI lifecycle, including planning, design, development, deployment, operation, and oversight. In doing so, it incorporates governance principles such as transparency, fairness, accountability, explainability, and risk management, translating these principles into operational processes, controls, and artefacts. These principles are consistent with the broader literature on trustworthy and responsible AI (Floridi et al., 2018; Jobin, Ienca and Vayena, 2019).

Governance-oriented maturity models represent a significant advancement over earlier deployment-focused approaches. They acknowledge that successful AI adoption requires more than technical capability and increasingly recognise the importance of legal compliance, ethical responsibility, and organisational accountability. In particular, these frameworks incorporate regulatory and ethical considerations, embed governance practices throughout the AI lifecycle, and provide mechanisms for operationalising high-level governance principles into practical governance activities (OECD, 2019; Mittelstadt, 2019).

Despite these contributions, important limitations remain. Governance-oriented models continue to conceptualise governance primarily as a collection of operational processes and controls rather than as an organisational capability that can be systematically developed, measured, and continuously improved. While they provide guidance on governance activities, they offer limited support for evaluating governance maturity, assessing governance effectiveness, or linking governance performance to broader organisational outcomes.

Furthermore, existing frameworks provide limited recognition of board-level governance and strategic accountability. Issues such as director oversight, governance reporting, assurance mechanisms, fiduciary responsibility, and strategic governance decision-making are generally absent or only implicitly addressed (Tricker, 2019; Mallin, 2019). Similarly, governance practices are rarely linked to measurable performance indicators, organisational capability development, or accountability frameworks that would enable organisations to evaluate governance effectiveness over time.

Consequently, although governance-oriented maturity models represent an important evolution in AI governance thinking, they remain largely operational in focus. They provide valuable guidance on governance processes but do not fully address governance as a strategic organisational capability that supports board oversight, performance measurement, accountability, and continuous improvement. This limitation highlights the need for a more comprehensive governance maturity model capable of integrating governance processes, organisational capabilities, and strategic governance objectives within a single framework.

Comparative Synthesis and Critical Limitations

A synthesis of the literature reveals two dominant streams of AI maturity assessment. The first comprises deployment-focused maturity models that emphasise technological capability, organisational readiness, and the successful adoption of AI systems (Schumacher, Erol and Sihn, 2016; Dwivedi, Y.K. et al., 2021). The second comprises governance-oriented frameworks that focus on ethical principles, risk management, security controls, accountability, and lifecycle governance processes (Floridi et al., 2018; Raji et al., 2020). Although both streams contribute valuable insights, neither provides a comprehensive mechanism for evaluating AI governance as a strategic organisational capability.

The analysis identifies four recurring limitations. First, existing models provide limited integration of board-level oversight and strategic accountability. Governance activities are typically positioned within operational or technical functions, with little consideration of director responsibilities, governance reporting, assurance mechanisms, or fiduciary oversight of AI-related risks (Tricker, 2019). This omission is increasingly significant given the growing expectation that boards play an active role in overseeing the governance of emerging technologies.

Second, there is a lack of measurable governance performance indicators. While many frameworks assess organisational capability, process maturity, or compliance activities, they provide limited means for evaluating whether governance mechanisms are achieving their intended objectives. As a result, organisations may be able to demonstrate the existence of governance structures without being able to assess their effectiveness or contribution to organisational outcomes (Wendler, 2012).

Third, governance remains fragmented across legal, technical, ethical, and organisational domains. Existing approaches often address these dimensions independently, resulting in siloed governance practices that may create inconsistencies between regulatory obligations, ethical expectations, and operational implementation (OECD, 2019; Mittelstadt, 2019). Such fragmentation limits the organisation's ability to establish a coherent and integrated governance framework.

Fourth, current models place limited emphasis on outcome-based evaluation. Measures relating to governance effectiveness, such as reductions in risk exposure, improvements in regulatory compliance, enhanced stakeholder trust, or organisational resilience, are largely absent from existing maturity assessments (Raji et al., 2020). Consequently, governance is frequently evaluated in terms of activities and controls rather than organisational impact.

Taken together, these limitations suggest that existing maturity models do not adequately conceptualise AI governance as a measurable organisational capability. Instead, governance is generally treated as a collection of processes, controls, or compliance activities rather than as a strategic capability that can be assessed, monitored, and continuously improved. This gap provides the foundation for the development of the AI Governance Capability Maturity Model proposed in this study.

Research Gap and Theoretical Positioning

The preceding review demonstrates that existing AI maturity models provide valuable mechanisms for assessing organisational readiness, technological capability, and the operational deployment of AI systems. Similarly, emerging governance frameworks have strengthened organisational understanding of risk management, compliance, accountability, and lifecycle governance. However, despite these advances, the literature does not provide a comprehensive framework for assessing AI governance as a strategic organisational capability.

Several important limitations remain. Existing maturity models typically focus on AI adoption and operational performance rather than governance effectiveness. Governance-oriented frameworks, while providing guidance on governance processes and controls, rarely integrate legal, ethical, organisational, and technical dimensions within a unified assessment structure. Furthermore, current approaches provide limited support for board-level oversight, accountability, and assurance, despite growing regulatory expectations that directors oversee AI-related risks and governance outcomes. Equally significant is the absence of measurable governance indicators that enable organisations to evaluate governance performance, benchmark maturity, and monitor continuous

improvement over time.

These limitations reveal a fundamental gap in the literature: the absence of a maturity model that conceptualises AI governance as a measurable organisational capability linked to governance performance, accountability, and board-level oversight. Existing frameworks largely assess an organisation's ability to develop and deploy AI systems but provide limited insight into its capacity to govern those systems effectively throughout their lifecycle.

This study addresses that gap through the development of an AI Governance Capability Maturity Model that extends existing maturity approaches beyond technical deployment and operational readiness. The proposed model reconceptualises AI governance as an organisational capability that can be systematically developed, assessed, monitored, and continuously improved. In doing so, it integrates governance processes, organisational capabilities, maturity assessment, and performance measurement within a single framework.

The theoretical foundation for this approach is drawn from capability-based theory, which argues that sustainable organisational performance depends on an organisation's ability to integrate, coordinate, and adapt complex processes and resources in dynamic environments (Teece, 2007; Eisenhardt and Martin, 2000). Applying this perspective to AI governance shifts the focus from the existence of governance controls to the organisation's capability to implement, sustain, evaluate, and improve governance practices over time. This capability-based view provides the conceptual basis for the maturity model proposed in this study and positions AI governance as a strategic organisational function rather than a narrowly defined compliance activity.

Bridge to the Proposed Framework

To operationalise this contribution, the study builds upon an existing six-phase AI governance framework (Wong, 2025; Wong, 2026) and extends it into a structured capability and maturity model. This transformation enables governance processes to be evaluated not only in terms of their existence, but also in terms of their effectiveness, integration, and organisational impact.

METHODOLOGY

Research Approach

This study adopts a qualitative integrative synthesis methodology to develop a measurable AI governance capability maturity model. Integrative synthesis is appropriate where knowledge is dispersed across multiple domains and requires consolidation into a coherent conceptual framework (Wendler, 2012; Neely, Gregory and Platts, 2005). In the context of AI governance, relevant insights span legal, regulatory, organisational, and technical literatures, which are often fragmented and lack a unified analytical structure (OECD, 2019; Mittelstadt, 2019).

Consistent with prior theory-building research in governance and information systems, the study does not rely on primary empirical data. Instead, it systematically synthesises existing knowledge to construct a theoretically grounded and practically applicable model. This approach is particularly suitable given the emerging nature of AI governance, where conceptual clarity and integration remain underdeveloped (Floridi et al., 2018; Jobin, Ienca and Vayena, 2019).

Research Design

This study adopts an interpretive, theory-building research design to develop a governance capability maturity model for artificial intelligence. The research seeks to extend existing AI governance and maturity model literature by addressing a recognised gap in the evaluation of governance effectiveness. As identified in the literature review, current AI maturity models predominantly focus on technological capability, organisational readiness, or operational governance processes, but provide limited mechanisms for assessing governance as a measurable organisational capability (Sonntag et al., 2024).

The study builds upon two complementary foundations. The first is prior research examining the legal, ethical,

and organisational risks associated with the development and deployment of AI systems (Wong, 2025). The second is the development of a six-phase AI governance framework that structures governance activities across the AI lifecycle and provides a process-oriented foundation for operationalising governance practices (Wong, 2026).

Drawing on these foundations, the present research advances the literature by reconceptualising AI governance as an organisational capability that can be systematically developed, assessed, and continuously improved. Rather than evaluating governance solely in terms of the existence of policies, controls, or compliance activities, the proposed approach focuses on the organisation's ability to implement, integrate, monitor, and enhance governance practices over time. This perspective enables governance effectiveness to be assessed through maturity levels and measurable performance indicators, thereby linking governance activities to organisational outcomes.

The theoretical basis for this approach is grounded in capability-based theory, which posits that sustainable organisational performance depends upon an organisation's capacity to integrate, coordinate, and reconfigure resources and processes in response to changing environmental conditions (Teece, 2007; Eisenhardt and Martin, 2000). Applying this perspective to AI governance provides a foundation for evaluating governance maturity as a dynamic organisational capability rather than a static compliance function. This conceptualisation underpins the development of the AI Governance Capability Maturity Model proposed in this study.

Data Sources and Selection

The integrative synthesis draws upon three complementary categories of sources to capture the multidisciplinary nature of AI governance. Given that AI governance spans legal, ethical, technical, organisational, and regulatory domains, no single body of literature provides a sufficiently comprehensive foundation for model development. Accordingly, the study combines regulatory frameworks, legal sources, and academic literature to establish both conceptual breadth and practical relevance.

Regulatory and Standards Frameworks

The first category comprises internationally recognised AI governance frameworks and standards, including the National Institute of Standards and Technology AI Risk Management Framework (NIST, 2023), ISO/IEC 42001 Artificial Intelligence Management Systems (ISO, 2023), and the European Union Artificial Intelligence Act (European Union, 2024). These sources provide contemporary guidance on risk-based governance, accountability, transparency, assurance, and regulatory compliance. They were selected because they represent emerging benchmarks for organisational AI governance and increasingly influence both regulatory expectations and industry practice.

Legal and Doctrinal Sources

The second category consists of legal and doctrinal materials addressing issues relevant to AI governance, including privacy and data protection, liability, consumer protection, discrimination, accountability, and regulatory compliance. These sources establish the legal obligations that organisations must consider when developing and deploying AI systems and provide an important foundation for understanding governance from a compliance and risk management perspective (OECD, 2019; Raji et al., 2020). Incorporating legal sources ensures that the proposed framework reflects not only governance best practice but also emerging regulatory requirements.

Academic and Conceptual Literature

The third category comprises academic research relating to AI governance, organisational capability, maturity models, corporate governance, and technology risk management. These sources provide the theoretical foundations necessary for model development, including insights into governance structures, capability development, organisational performance, maturity assessment, and continuous improvement (Wendler, 2012; Sonntag et al., 2024). Academic literature was particularly important in informing the conceptualisation of AI governance as an organisational capability and in identifying mechanisms for assessing governance maturity.

Sources were selected using three criteria. First, they were required to demonstrate direct relevance to AI governance, organisational capability, maturity assessment, or related governance disciplines. Second, priority was given to peer-reviewed academic publications, recognised standards, and authoritative institutional reports to ensure credibility and reliability. Third, emphasis was placed on literature published after 2018 to reflect the rapid evolution of AI governance frameworks, regulatory developments, and emerging industry practices.

This selection strategy ensures that the resulting framework is informed by both theoretical and practical perspectives, integrates legal and organisational dimensions of governance, and remains aligned with contemporary regulatory and governance expectations. The combination of these diverse source categories provides a robust foundation for the development of an AI Governance Capability Maturity Model that is both conceptually rigorous and practically applicable.

Analytical Process

The development of the proposed AI Governance Capability Maturity Model followed a structured three-stage analytical process designed to transform fragmented governance concepts into an integrated and assessable governance framework. The process combines literature synthesis, framework integration, and capability modelling to establish a systematic foundation for maturity assessment.

Stage 1: Governance Mechanism Extraction and Coding

The first stage involved the identification, extraction, and coding of governance mechanisms reported across the literature. Particular attention was given to governance activities relating to risk management, legal and regulatory compliance, ethical oversight, accountability, assurance, and organisational control. Examples of coded mechanisms included risk classification and assessment processes, compliance management practices, auditing and assurance activities, governance reporting structures, and board oversight arrangements.

The purpose of this stage was to identify recurring governance themes and establish a consolidated set of governance elements that transcended disciplinary boundaries. Through this process, governance concepts originating from legal, organisational, technical, and management perspectives were synthesised into a common analytical framework (Neely, Gregory and Platts, 2005).

Stage 2: Framework Integration

The second stage involved mapping the extracted governance mechanisms onto the six-phase AI governance framework developed in prior research (Wong, 2026). This process enabled diverse governance activities to be organised into a coherent lifecycle structure encompassing strategic governance, risk assessment, data governance, AI development and deployment, continuous monitoring, and accountability.

By integrating governance mechanisms within a common process architecture, the framework established a consistent representation of governance activities across the AI lifecycle. This step reduced fragmentation within the literature and ensured that governance practices could be examined as interconnected components of a broader governance system rather than as isolated controls or compliance activities.

Stage 3: Capability and Maturity Model Development

The final stage reinterpreted the integrated governance framework through a capability-based perspective. Rather than viewing governance as a collection of discrete processes, governance activities were conceptualised as organisational capabilities that can be developed, measured, and continuously improved over time. These capabilities were subsequently structured into a five-level maturity model, providing a mechanism for evaluating governance capability at different stages of organisational development.

This stage also introduced measurable dimensions of governance by linking governance processes to capability outcomes and performance indicators. The resulting framework enables organisations to assess governance maturity, identify capability gaps, benchmark performance, and monitor governance improvement over time.

Collectively, the three-stage analytical process transforms AI governance from a procedural and compliance-oriented construct into a capability-based framework for organisational assessment and continuous improvement. This transformation is consistent with capability-based theories of the firm, which emphasise the role of organisational capabilities in supporting performance, adaptability, and long-term competitive advantage (Teece, 2007). The resulting maturity model therefore provides both a conceptual and practical mechanism for evaluating AI governance capability across the organisation.

Methodological Rationale

An integrative synthesis methodology is particularly appropriate for this study because AI governance is inherently multidisciplinary and characterised by a fragmented body of literature. Existing research approaches AI governance from a variety of perspectives, including legal compliance, ethical principles, technical controls, risk management, and organisational governance. While each perspective provides valuable insights, the literature lacks a comprehensive framework that integrates these dimensions into a coherent approach for assessing and improving governance capability (Mittelstadt, 2019; OECD, 2019).

The fragmented nature of the field presents a significant challenge for organisations seeking to implement effective AI governance. Regulatory frameworks emphasise legal compliance and accountability, ethical frameworks focus on responsible and trustworthy AI, while technical and management frameworks concentrate on operational controls and risk mitigation. As a result, organisations often adopt governance practices that are disconnected, difficult to measure, and challenging to align with broader organisational objectives.

The integrative synthesis approach addresses this challenge by systematically combining insights from these diverse streams of literature. Through this process, common governance themes, processes, and capability requirements can be identified and consolidated into a unified conceptual framework. This enables the development of a governance model that moves beyond isolated governance mechanisms and instead treats governance as an organisational capability that can be developed, assessed, and continuously improved.

Furthermore, the methodology supports the translation of abstract governance principles into practical and measurable organisational constructs. By integrating governance processes, capability theory, maturity model concepts, and performance measurement approaches, the study establishes a foundation for evaluating governance effectiveness in a structured and repeatable manner.

This approach is consistent with established theory-building and maturity model development methodologies, which emphasise the synthesis of existing knowledge to create integrated conceptual frameworks capable of both advancing theory and informing practice (Wendler, 2012). Consequently, the methodology provides a robust foundation for the development of an AI Governance Capability Maturity Model that is both theoretically grounded and practically applicable across a range of organisational contexts.

Link to Model Development

The methodological approach adopted in this study directly informs the development of the AI Governance Capability Maturity Model presented in Section 4. Through the integrative synthesis of the literature, three key conceptual foundations emerged that collectively shape the proposed framework.

First, the six-phase AI governance framework identified in prior research provides the structural foundation of the model (Wong, 2026). The framework captures the key governance activities required across the AI lifecycle and establishes a process-oriented view of AI governance that extends beyond technical development and deployment activities.

Second, the reinterpretation of AI governance through a capability-based lens provides the theoretical basis for assessing governance maturity. Drawing on capability theory, governance is conceptualised as an organisational capability that can be developed, measured, and continuously improved over time (Teece, 2007). This perspective shifts the focus from the existence of governance controls to the organisation's ability to consistently implement and sustain effective governance practices.

Third, the incorporation of maturity model principles provides a mechanism for evaluating governance capability at different levels of organisational development. By introducing structured maturity levels, the framework enables organisations to assess their current governance capability, identify capability gaps, benchmark performance, and establish pathways for continuous improvement.

Together, these elements provide the foundation for translating the findings of the literature review into an operational governance capability model. The resulting framework integrates governance processes, organisational capabilities, maturity assessment, and performance measurement within a single structure, thereby providing a systematic approach for evaluating and improving AI governance capability across the organisation.

Proposed AI Governance Maturity Model

Identified Gaps in Existing Maturity Approaches

The literature review identified two dominant streams of AI maturity assessment. The first comprises deployment-focused maturity models that evaluate organisational readiness, technological capability, and the extent of AI adoption. The second comprises governance-oriented frameworks that focus on risk management, compliance, accountability, and lifecycle controls (Sonntag et al., 2024; Wendler, 2012). While both streams make valuable contributions to understanding AI implementation and governance, neither provides a comprehensive mechanism for assessing AI governance as a strategic organisational capability.

Deployment-focused models typically demonstrate strong capability in assessing the development, deployment, and operationalisation of AI technologies. However, they generally provide limited attention to governance structures, accountability mechanisms, legal compliance, and board oversight. Conversely, governance-oriented frameworks provide guidance on governance processes and lifecycle controls but often lack mechanisms for measuring governance capability, evaluating governance maturity, or linking governance performance to organisational outcomes (Dwivedi, Y.K. et al., 2021; Raji et al., 2020).

To illustrate these differences, Table 1 synthesises the strengths and limitations of both streams across six governance dimensions.

Table 1: A synthesis of both streams highlighting six key dimensions of comparison

Area	**Deployment Models**	**Governance-Oriented Models (e.g., AIMA)**	**Identified Gap**
AI capability	Strong	Moderate	—
Governance processes	Weak	Strong	Partial integration
Board-level oversight	Absent	Absent	Major gap
Measurement of governance	Weak	Limited	Critical gap
Strategic governance integration	Absent	Limited	Major gap
Outcome-based metrics	Absent	Absent	Critical gap

The analysis highlights several important shortcomings in current literature. Although governance processes are increasingly recognised as important components of AI management, they are typically treated as supporting mechanisms rather than as organisational capabilities that can be systematically developed, measured, and improved. As a result, existing frameworks provide limited guidance regarding how organisations can evaluate governance effectiveness or demonstrate governance maturity over time.

Two deficiencies are particularly significant. First, there is limited recognition of board-level oversight and strategic accountability. Despite growing regulatory and governance expectations that boards oversee AI-related

risks, existing maturity models provide little guidance on governance reporting, assurance mechanisms, director accountability, or the integration of AI governance within broader corporate governance structures (Tricker, 2019; Mallin, 2019; OECD, 2019).

Second, current models provide few mechanisms for measuring governance performance. While many frameworks prescribe governance principles, controls, or processes, they rarely include measurable indicators that enable organisations to assess governance effectiveness, benchmark performance, or monitor improvement over time (Wendler, 2012; Neely, Gregory and Platts, 2005). This limitation reduces their practical value as governance management and assurance tools.

Collectively, these gaps suggest that existing maturity approaches do not adequately conceptualise AI governance as an organisational capability that can be evaluated, monitored, and continuously improved. This limitation provides the motivation for the development of the AI Governance Capability Maturity Model proposed in this study, which seeks to integrate governance processes, capability development, maturity assessment, performance measurement, and board-level oversight within a single framework.

Mapping Existing Models to the Six-Phase Governance Framework

To further evaluate the limitations of existing AI maturity models, the models identified in the literature were mapped against the six-phase AI governance framework developed in prior research (Wong, 2025; Wong, 2026). The framework encompasses six governance phases: Strategic Alignment and Governance Foundations; Risk Identification and Legal-Ethical Assessment; Data Governance and Infrastructure Control; AI Development and Deployment Governance; Monitoring, Evaluation and Continuous Assurance; and Accountability, Audit and Continuous Improvement. Mapping existing models against these phases provides a structured basis for assessing the extent to which current maturity frameworks address governance requirements across the AI lifecycle.

Table 2: Existing maturity models

Governance Phase	**Coverage in Existing Models**	**Gap Identified**	**Contribution of Proposed Framework**
Strategic Alignment & Governance Foundations	Partial	Lack of board-level oversight and governance structures	Introduces explicit board accountability and governance roles
Risk Identification & Legal-Ethical Assessment	Limited	Absence of systematic legal and ethical risk assessment	Integrates regulatory compliance and ethical AI frameworks
Data Governance & Infrastructure Control	Moderate	Data treated as technical rather than governed asset	Embeds privacy, security, and data governance principles
AI Development & Deployment Governance	Strong	Focus on capability without accountability	Introduces governance checkpoints and auditability
Monitoring, Evaluation & Continuous Assurance	Weak	Limited lifecycle monitoring and feedback mechanisms	Establishes continuous monitoring and assurance processes
Accountability, Audit & Continuous Improvement	Minimal	No clear accountability or audit integration	Embeds audit, responsibility frameworks, and governance feedback loops

The mapping reveals a significant imbalance in the focus of existing maturity models. Most frameworks provide substantial coverage of AI development and deployment activities, reflecting a strong emphasis on technological

capability and organisational readiness for AI adoption (Sonntag et al., 2024). Strategic considerations are addressed to a lesser extent, while governance activities relating to risk assessment, assurance, accountability, and continuous improvement receive comparatively limited attention.

This imbalance creates several important governance deficiencies. First, accountability mechanisms are often weak or absent, with limited guidance regarding governance roles, responsibilities, and board oversight (Tricker, 2019). Second, continuous governance activities such as monitoring, auditing, assurance, and performance evaluation are underdeveloped, reducing the organisation's ability to identify emerging risks and adapt governance practices over time (Raji et al., 2020). Third, the integration of legal, regulatory, and ethical requirements remains fragmented, resulting in governance approaches that may not adequately address the increasingly complex compliance obligations associated with AI deployment (OECD, 2019; Mittelstadt, 2019).

These findings support a central argument of this study: existing AI maturity models are necessary but insufficient for effective AI governance. While they provide valuable mechanisms for assessing AI capability and organisational readiness, they do not adequately evaluate whether AI systems are governed in a manner that is accountable, legally compliant, ethically responsible, and subject to ongoing assurance. The proposed governance capability maturity model addresses this gap by extending maturity assessment beyond technical capability to encompass the governance processes, organisational structures, accountability mechanisms, and performance measures required for responsible AI adoption.

Conceptualising AI Governance as Organisational Capability

To address the limitations of existing AI governance approaches, this study reconceptualises AI governance as an organisational capability rather than a collection of discrete policies, controls, or compliance activities. While many governance frameworks focus on the existence of governance mechanisms, they provide limited insight into an organisation's ability to consistently apply, adapt, and improve those mechanisms in response to evolving technological, regulatory, and organisational challenges.

This perspective is grounded in capability-based theory, which argues that sustainable organisational performance arises from the ability to integrate, coordinate, and continuously enhance complex organisational processes and resources (Teece, 2007; Eisenhardt and Martin, 2000). From this viewpoint, governance capability extends beyond the presence of formal structures and procedures to encompass the organisation's capacity to deploy governance mechanisms effectively and to adapt them as circumstances change.

Accordingly, AI governance capability can be defined as an organisation's ability to establish, implement, monitor, and continuously improve governance mechanisms that ensure the responsible development, deployment, and use of artificial intelligence. This capability includes the capacity to systematically identify and manage AI-related risks, integrate legal, ethical, technical, and organisational governance requirements, evaluate governance performance through measurable indicators, and maintain accountability through appropriate organisational and board-level oversight (OECD, 2019; Floridi et al., 2018; Jobin, Ienca and Vayena, 2019; Neely, Gregory and Platts, 2005; Tricker, 2019).

Viewing AI governance through a capability lens provides several advantages. First, it recognises governance as a dynamic and evolving organisational competence rather than a static compliance function. Second, it enables governance effectiveness to be assessed in terms of maturity and performance, rather than merely the existence of policies or controls. Third, it establishes a foundation for continuous improvement by recognising that governance capabilities can be developed, measured, and strengthened over time.

This reconceptualisation forms the theoretical foundation of the proposed maturity model. By treating governance as an organisational capability, the model provides a structured mechanism for assessing governance maturity, identifying capability gaps, and guiding the development of more effective and sustainable AI governance practices.

AI Governance Maturity Model

Building on the six-phase framework, the proposed model (Table 3) introduces a five-level maturity structure

that captures the progression of AI governance capability from fragmented and reactive practices to fully integrated, strategic governance (Wendler, 2012; Schumacher, Erol and Sihn, 2016).

Table 3: Proposed model

Level	Maturity Stage	Description
Level 1	Initial / Ad hoc	AI governance is informal, fragmented, and unmanaged
Level 2	Developing	Basic policies exist but are inconsistently applied
Level 3	Defined	Governance processes are formalised and repeatable
Level 4	Managed	Governance is monitored, measured, and integrated into decision-making
Level 5	Optimised	Governance is embedded, continuously improved, and aligned with strategy

Unlike traditional maturity models, this framework evaluates not only capability development, but also governance effectiveness, particularly in relation to accountability, compliance, and continuous oversight (Sonntag et al., 2024).

AI Governance Capability Scoring Matrix

To operationalise the maturity model, governance capability is assessed across six phases using a five-level scale. This enables organisations to evaluate both the presence and effectiveness of governance mechanisms.

The scoring matrix (Table 4) defines progressive capability across each governance phase, from ad hoc practices to fully integrated governance systems, consistent with established performance measurement approaches (Kaplan and Norton, 1996; Neely, Gregory and Platts, 2005).

Table 4: AI Governance Maturity Scoring Matrix

Governance Phase	Level 1: Initial	Level 2: Developing	Level 3: Defined	Level 4: Managed	Level 5: Optimised
1. Strategic Alignment and Governance Foundations	AI projects are initiated without clear governance or board visibility.	AI strategy exists in limited areas, but oversight is informal.	AI governance roles, policies, and reporting lines are documented.	Board and senior management receive regular AI governance reporting.	AI governance is embedded in corporate strategy, risk appetite, and board oversight.
2. Risk Identification and Legal-Ethical Assessment	Legal, ethical, and regulatory risks are considered only after issues arise.	Some risk assessments are conducted for high-risk AI use cases.	Formal AI risk assessments include privacy, discrimination, transparency, and compliance issues.	Legal and ethical risk assessments are routinely reviewed and updated.	Risk assessment is continuous, predictive, and integrated with enterprise risk management.
3. Data Governance and Infrastructure Control	Data used for AI is poorly documented and inconsistently	Basic data quality, privacy, and security controls exist.	Data governance standards are applied to AI datasets and	Data controls are tested, monitored, and subject to	Data governance is proactive, auditable, privacy-by-design, and

	controlled.		model inputs.	assurance.	aligned with regulatory expectations.
4. AI Development and Deployment Governance	AI models are developed or adopted without consistent approval processes.	Some testing or validation occurs before deployment.	AI development follows documented approval, validation, and deployment procedures.	Deployment decisions are supported by explainability, testing, and audit trails.	AI deployment is governed through lifecycle controls, human oversight, and continuous assurance.
5. Monitoring, Evaluation and Continuous Assurance	AI performance is not systematically monitored after deployment.	Monitoring occurs reactively or for selected systems only.	AI systems are periodically reviewed for performance, bias, reliability, and compliance.	Monitoring results are reported to management and used to improve controls.	Continuous monitoring detects drift, bias, harm, and compliance risks in real time or near real time.
6. Accountability, Audit and Continuous Improvement	No clear accountability exists for AI outcomes or failures.	Accountability is assigned informally or only at project level.	Roles and responsibilities are formally assigned across business, technical, legal, and risk functions.	Internal audit, compliance, and risk functions review AI governance effectiveness.	Accountability is embedded through audit, board oversight, stakeholder reporting, and continuous improvement.

Measurement and Scoring Approach

The proposed model can be operationalised through a structured scoring methodology in which each governance phase is assessed against the five maturity levels described in the framework. Scores are assigned on a five-point scale, ranging from Level 1 (Initial) to Level 5 (Optimised), reflecting the extent to which governance capabilities are established, implemented, measured, and continuously improved.

An overall AI Governance Maturity Score can then be calculated by averaging the maturity scores across the six governance phases:

$$\text{AI Governance Maturity Score} = \frac{\sum \text{Phase Scores}}{6}$$

This approach provides both a holistic assessment of organisational governance maturity and a diagnostic mechanism for identifying strengths and weaknesses across different areas of governance. While the overall maturity score offers a high-level indicator of governance capability, phase-level scores enable more detailed analysis of specific governance functions and areas requiring improvement.

The scoring framework recognises that governance maturity is rarely uniform across an organisation. For example, an organisation may demonstrate advanced capabilities in AI development, deployment, and operational management while exhibiting lower levels of maturity in accountability, assurance, auditing, or regulatory compliance. Such variations are important because technical sophistication does not necessarily translate into effective governance or risk management. By providing visibility of these differences, the model enables organisations to prioritise governance investments, target capability development initiatives, and monitor improvement over time (Kaplan and Norton, 1996).

Furthermore, the scoring approach supports benchmarking, trend analysis, and board-level reporting by providing a consistent and repeatable mechanism for evaluating governance performance. As organisations progress through the maturity levels, changes in scores can be used to demonstrate governance improvement and support evidence-based decision-making regarding AI governance priorities and resource allocation.

Contribution of the Model

The proposed AI governance capability maturity model advances the existing literature on AI governance and maturity assessment in several important respects.

First, it extends traditional maturity model approaches by shifting the focus from the maturity of AI technologies and organisational capabilities to the maturity of governance itself. While prior studies have largely concentrated on organisational readiness and AI adoption capabilities (Sonntag et al., 2024), the proposed model emphasises the structures, processes, and controls required to govern AI responsibly throughout its lifecycle.

Second, the model adopts a holistic governance perspective by integrating legal, ethical, technical, and organisational dimensions within a single assessment framework. Existing governance approaches frequently address these dimensions independently, creating the risk of fragmented governance practices and inconsistent implementation. By bringing together regulatory obligations, ethical principles, technical controls, and organisational governance mechanisms, the model provides a more comprehensive approach to managing AI-related risks and responsibilities (Floridi et al., 2018; OECD, 2019).

Third, the model incorporates a measurement architecture that enables governance capability to be assessed using objective and observable indicators. Through the use of input, process, output, and outcome metrics, organisations can evaluate governance implementation, monitor performance over time, and assess the effectiveness of governance interventions. This addresses a recognised limitation in many governance frameworks, which provide principles and guidance but offer limited mechanisms for performance measurement and evaluation (Neely, Gregory and Platts, 2005).

Fourth, the model strengthens the connection between operational governance and board-level oversight. By linking maturity assessment to governance dashboards, reporting structures, and assurance processes, it provides directors and senior executives with decision-relevant information that supports accountability, risk oversight, and strategic decision-making (Tricker, 2019).

Finally, the model is aligned with emerging international AI governance frameworks and regulatory developments, including the National Institute of Standards and Technology AI Risk Management Framework (NIST, 2023), ISO/IEC 42001 Artificial Intelligence Management Systems (ISO, 2023), and the European Union Artificial Intelligence Act (European Union, 2024). This alignment enhances the practical relevance of the framework and supports its application within increasingly complex regulatory environments.

Collectively, these contributions position the model as a theoretically grounded and practically applicable framework for assessing and improving AI governance capability. By linking governance processes, organisational capabilities, maturity assessment, and performance measurement, the model provides a structured mechanism for transforming AI governance from a compliance-oriented activity into a strategic organisational capability that supports responsible innovation, regulatory compliance, and sustainable value creation.

Measurement and Operationalisation Of Ai Governance Capability

From Maturity Model to Measurable Governance

This section operationalises the AI governance capability maturity model presented in Section 4 by defining a structured measurement framework. The objective is to enable organisations to systematically evaluate governance capability across the six governance phases and five maturity levels.

The measurement framework translates governance capability into observable and assessable indicators, allowing organisations to assess both the implementation of governance mechanisms and their effectiveness in

practice.

In doing so, the model provides a basis for consistent evaluation, comparison, and monitoring of governance performance across organisational contexts. This supports the practical application of the maturity model as a tool for governance assessment, benchmarking, and continuous improvement.

The framework is aligned with established performance measurement approaches, which emphasise the importance of linking organisational processes to measurable outcomes (Kaplan and Norton, 1996; Neely, Gregory and Platts, 2005).

Measurement Architecture

The measurement architecture assesses AI governance capability across four complementary dimensions: input, process, output, and outcome metrics. Collectively, these dimensions provide a comprehensive framework for evaluating both the implementation of governance mechanisms and their organisational impact across the AI lifecycle.

Input Metrics (Governance Foundations)

Input metrics assess the organisational resources, structures, and capabilities required to support effective AI governance. Typical measures include the existence of governance policies and standards, clearly defined roles and responsibilities, governance committee structures, staff training and competency development, and the allocation of financial and technological resources. These indicators reflect the extent to which governance foundations have been established to support responsible AI adoption.

Process Metrics (Governance Execution)

Process metrics evaluate the effectiveness with which governance mechanisms are implemented and operated. Examples include the proportion of AI systems subjected to risk classification, the frequency of bias and fairness assessments, implementation rates of compliance-by-design controls, the conduct of internal audits and reviews, and the effectiveness of incident response procedures. These measures provide insight into governance execution and control effectiveness, consistent with established risk management and assurance practices (OECD, 2019; Raji et al., 2020).

Output Metrics (Governance Artefacts)

Output metrics measure the tangible deliverables generated through governance activities. Examples include the number of AI systems supported by model cards or equivalent documentation, completed audit and compliance reports, maintained risk registers and mitigation plans, and transparency or explainability reports. Such artefacts demonstrate the operationalisation of governance principles, particularly transparency, accountability, and traceability (Floridi et al., 2018; Jobin, Ienca and Vayena, 2019).

Outcome Metrics (Governance Effectiveness)

Outcome metrics assess whether governance activities achieve their intended objectives and contribute to organisational performance. Examples include reductions in compliance breaches, decreases in the number and severity of AI-related incidents, favourable regulatory findings, improved stakeholder trust indicators, and alignment with environmental, social, and governance (ESG) objectives. These measures provide evidence of governance effectiveness and long-term organisational value creation (Mittelstadt, 2019; Neely, Gregory and Platts, 2005).

Together, these four categories provide a balanced measurement framework that enables organisations to evaluate governance capability from foundational readiness through to operational performance and strategic outcomes.

Linking Measurement to Maturity Levels

A key contribution of this framework is the explicit linkage between measurement capability and governance maturity. As organisations progress through maturity levels, their ability to measure and manage governance also evolves.

Maturity Level	Measurement Capability
Level 1: Ad hoc	No formal metrics; limited visibility
Level 2: Developing	Basic compliance tracking and reporting
Level 3: Defined	Risk-based metrics and structured monitoring
Level 4: Managed	Integrated dashboards and performance tracking
Level 5: Optimised	Predictive, real-time, and strategic metrics

This progression reflects the evolution from reactive governance to proactive, data-driven oversight, consistent with maturity model theory (Wendler, 2012; Sonntag et al., 2024).

Board-Level Governance Dashboard

To facilitate effective oversight and informed decision-making, governance metrics should be consolidated into a board-level dashboard that provides directors with a clear and concise view of AI governance performance, risk exposure, and organisational maturity. By translating complex technical, legal, and operational information into decision-relevant indicators, the dashboard supports board accountability, strategic oversight, and risk governance.

The dashboard should present a balanced set of leading and lagging indicators drawn from the governance measurement architecture. Typical indicators may include the proportion of AI systems classified according to risk level, governance coverage across the AI lifecycle, the number and severity of unresolved governance issues, audit completion rates and associated findings, compliance performance, incident trends, and measures of regulatory exposure. Where appropriate, these indicators may be benchmarked against organisational targets, risk tolerances, and industry standards to enable trend analysis and performance evaluation.

In addition to providing visibility of governance performance, the dashboard supports proactive risk management by highlighting emerging issues requiring board attention. This enables directors to monitor whether governance controls remain effective as AI adoption expands and regulatory requirements evolve. The dashboard therefore functions as a strategic governance instrument, linking operational governance activities with board-level accountability and oversight responsibilities (Tricker, 2019; Mallin, 2019).

The proposed approach aligns with contemporary governance and assurance frameworks that emphasise transparency, accountability, and continuous monitoring of AI-related risks. These include the National Institute of Standards and Technology AI Risk Management Framework (NIST, 2023), International Organization for Standardization ISO/IEC 42001 (ISO, 2023), and the European Union AI Act, all of which place significant emphasis on governance oversight, accountability, and ongoing performance monitoring.

Integration with the Capability Framework

The measurement framework is directly aligned with the six-phase governance model and corresponding capability domains:

Governance Phase	Capability Domain
Strategic alignment	Regulatory intelligence

Risk identification	AI risk assessment
Compliance-by-design	Governance-by-design
Organisational capability	Governance capability and culture
Monitoring and assurance	Continuous assurance
Accountability and audit	External accountability and trust

This alignment ensures that governance measurement is not treated as a separate activity, but as an integral component of organisational capability development, consistent with capability-based theory (Teece, 2007).

Conceptual Integration

The measurement architecture completes the proposed AI governance capability model by integrating governance processes, organisational capabilities, maturity assessment, and performance measurement into a unified framework. Within this framework, governance processes provide the operational mechanisms through which AI risks are identified, assessed, monitored, and controlled. These processes collectively develop governance capabilities that reflect the organisation's capacity to manage AI responsibly and consistently across the AI lifecycle.

The maturity model provides a structured mechanism for evaluating the extent to which these capabilities are institutionalised, enabling organisations to benchmark current performance, identify capability gaps, and define pathways for continuous improvement. The measurement framework complements this assessment by providing objective indicators that monitor governance implementation, operational effectiveness, and organisational outcomes.

Together, these elements establish a layered governance architecture in which processes drive capability development, capabilities underpin maturity progression, and measurement provides evidence of governance effectiveness. This integration transforms AI governance from a collection of isolated compliance activities into a strategic organisational capability that supports responsible innovation, risk management, and regulatory compliance.

At the highest level, governance performance is embedded within board oversight and enterprise governance structures. Through the use of governance dashboards, assurance mechanisms, and performance reporting, directors are provided with decision-relevant information that supports accountability, strategic decision-making, and effective oversight of AI-related risks and opportunities (Tricker, 2019). The resulting framework therefore links operational governance activities with organisational strategy, enabling boards to exercise informed stewardship over the adoption and use of artificial intelligence.

DISCUSSION AND CONTRIBUTIONS

AI Governance as an Organisational Capability

The principal contribution of this study is the reconceptualisation of AI governance as an organisational capability rather than a collection of policies, controls, or compliance activities. Existing AI maturity models primarily assess technological readiness and deployment capability, while governance frameworks focus on governance processes and controls. Neither perspective adequately explains how organisations can evaluate their ability to govern AI effectively over time.

Drawing on capability-based theory, the proposed framework positions AI governance as a dynamic organisational competence that encompasses the ability to establish, implement, monitor, and continuously improve governance mechanisms across the AI lifecycle. This perspective shifts the focus from governance design to governance performance, enabling organisations to assess not only whether governance mechanisms exist, but also whether they operate effectively and contribute to organisational objectives. In doing so, the study

extends existing AI governance literature by providing a theoretical foundation for evaluating governance capability as a measurable organisational construct.

Integrating Governance, Maturity, and Measurement

A second contribution is the integration of governance processes, maturity assessment, and performance measurement within a single framework. Existing governance frameworks typically prescribe governance principles and controls but provide limited guidance on how governance effectiveness should be evaluated. Similarly, maturity models often assess organisational readiness without measuring governance outcomes.

The proposed framework addresses this limitation through a structured maturity model supported by a measurement architecture comprising input, process, output, and outcome metrics. This enables organisations to assess governance capability across multiple dimensions, benchmark performance, identify capability gaps, and monitor improvement over time. By linking governance activities to measurable indicators, the framework transforms governance from a largely descriptive concept into an evaluative and evidence-based management practice.

Strengthening Board-Level Oversight and Accountability

A third contribution is the explicit integration of board-level oversight within the governance maturity framework. As AI systems increasingly influence organisational performance, risk exposure, and regulatory compliance, boards are expected to exercise informed oversight of AI-related risks and governance arrangements. However, existing AI maturity models provide limited support for governance reporting, assurance, and director accountability.

The proposed framework addresses this gap by linking governance maturity and performance measurement to board-level dashboards, assurance mechanisms, and governance reporting structures. This enables directors to monitor governance effectiveness, evaluate organisational risk exposure, and make informed strategic decisions regarding AI adoption and oversight. The framework therefore bridges the gap between operational AI governance and enterprise governance, supporting a more accountable and strategically aligned approach to AI management.

Collectively, these contributions extend existing maturity model research beyond AI deployment capability and establish a foundation for evaluating AI governance as a measurable organisational capability. By integrating governance processes, maturity assessment, performance measurement, and board oversight within a single framework, the model provides a structured mechanism for supporting responsible AI adoption, regulatory compliance, and organisational accountability.

CONCLUSION

The rapid adoption of Artificial Intelligence has created an urgent need for governance approaches that extend beyond technical implementation and regulatory compliance. While existing maturity models provide valuable mechanisms for assessing AI capability and organisational readiness, and governance frameworks offer guidance on risk management and accountability, both provide limited support for evaluating governance effectiveness and organisational governance capability.

This study addresses that limitation through the development of an AI Governance Capability Maturity Model that reconceptualises AI governance as a measurable organisational capability. Drawing on capability-based theory, the framework integrates governance processes, maturity assessment, performance measurement, and board-level oversight within a unified governance architecture. The model extends existing approaches by enabling organisations to assess governance capability systematically, identify areas for improvement, and monitor governance performance over time.

The study makes three principal contributions. First, it provides a theoretical foundation for understanding AI governance as an organisational capability. Second, it introduces a structured maturity and measurement framework that enables governance effectiveness to be evaluated using observable indicators. Third, it

establishes a mechanism for linking governance performance to board-level oversight through dashboards, reporting structures, and assurance processes.

Together, these contributions position AI governance as a strategic organisational capability rather than a purely compliance-oriented function. The framework supports responsible AI adoption by enabling organisations to strengthen accountability, improve risk management, enhance regulatory compliance, and build stakeholder trust.

Although the model remains conceptual and requires empirical validation across different organisational and industry contexts, it provides a robust foundation for future research and practical implementation. As AI becomes increasingly embedded within organisational decision-making and business operations, the ability to measure, monitor, and continuously improve governance capability will become a critical component of effective corporate governance. The framework proposed in this study offers a structured pathway for achieving that objective and for strengthening board stewardship of artificial intelligence in an increasingly complex technological and regulatory environment.

REFERENCES

1. Australian Institute of Company Directors (AICD) (2024) Governing Artificial Intelligence: Guidance for Boards. Sydney: AICD.
2. Eisenhardt, K.M. and Martin, J.A. (2000) 'Dynamic capabilities: What are they?', *Strategic Management Journal*, 21(10–11), pp. 1105–1121.
3. Dwivedi, Y.K. et al. (2021) 'Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy', *International Journal of Information Management*, 57, Article 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002
4. 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).* Official Journal of the European Union, Brussels.
5. Floridi, L. et al. (2018) 'AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations', *Minds and Machines*, 28(4), pp. 689–707.
6. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2023) *ISO/IEC 42001:2023 Artificial intelligence — Management system requirements.* Geneva: ISO.
7. Jobin, A., Ienca, M. and Vayena, E. (2019) 'The global landscape of AI ethics guidelines', *Nature Machine Intelligence*, 1(9), pp. 389–399.
8. Kaplan, R.S. and Norton, D.P. (1996) The balanced scorecard: Translating strategy into action. Boston: Harvard Business School Press.
9. Mallin, C.A. (2019) Corporate Governance. 6th edn. Oxford: Oxford University Press.
10. Mittelstadt, B. (2019) 'Principles alone cannot guarantee ethical AI', *Nature Machine Intelligence*, 1(11), pp. 501–507.
11. National Institute of Standards and Technology (NIST) (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST.
12. Neely, A., Gregory, M. and Platts, K. (2005) 'Performance measurement system design: A literature review and research agenda', *International Journal of Operations & Production Management*, 25(12), pp. 1228–1263.
13. OECD (2019) OECD Principles on Artificial Intelligence. Paris: OECD.
14. Raji, I.D. et al. (2020) 'Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAccT '20)*, pp. 33–44.
15. Schumacher, A., Erol, S. and Sihn, W. (2016) 'A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises', Procedia CIRP, 52, pp. 161–166.
16. Sonntag, M., Mehmann, S., Mehmann, J. and Teuteberg, F. (2024) 'Development and evaluation of a maturity model for AI deployment capability of manufacturing companies', Information Systems Management, 42(1), pp. 37–67. doi:10.1080/10580530.2024.2319041
17. Teece, D.J. (2007) 'Explicating dynamic capabilities: The nature and microfoundations of (sustainable)

enterprise performance', Strategic Management Journal, 28(13), pp. 1319–1350.
18. Tricker, B. (2019) Corporate Governance: Principles, Policies, and Practices. 4th edn. Oxford: Oxford University Press.
19. Wendler, R. (2012) 'The maturity of maturity model research: A systematic mapping study', Information and Software Technology, 54(12), pp. 1317–1339.
20. 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
21. 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/
22. Wong, B. (2026a). *Human-Centred Governance for Responsible AI Adoption: Enabling Sustainable Business Transformation and Societal Value*. Accepted for presentation at the 17th International Conference on Applied Human Factors and Ergonomics (AHFE 2026), Istanbul, Türkiye, 20–24 July 2026.