

# AI Governance and Ethical Frameworks in Digital Enterprises: A CIO-Centric Governance Model

*Dr. Jipson George Thoomkuzhy<sup>1</sup>, Dr. Abeer Ahmed Aljohani<sup>2</sup>*

<sup>1</sup> Lincoln University College Malaysia; <sup>2</sup> Applied College, Taibah University, Madinah, Saudi Arabia

Email ID: jipsongearge2000@gmail.com

---

**Abstract:** Artificial Intelligence (AI) has become an integral and unavoidable part of modern digital businesses. It helps businesses with automation, predictive analytics, and decision-making. However, the rapid rise of AI has outpaced the development of governance, leading to challenges in ethics, operations, and leadership. Guidelines such as the European Union AI Act (European Union, 2024), ISO/IEC 42001 (ISO/IEC, 2023), and the NIST AI Risk Management Framework (NIST, 2023) offer important insights but do not clearly define the executive leadership roles required for AI governance. The Chief Information Officer (CIO), who oversees enterprise IT governance, is vital in ensuring the ethical and compliant use of AI. Yet, there is little research on CIO skills, governance duties, and leadership models specific to AI. This paper aims to lay the foundation for developing a CIO-focused AI governance framework using a sequential, exploratory, mixed-methods approach. The qualitative phase will investigate executive governance views, followed by quantitative validation among IT governance professionals. This research aims to close the gap in leadership and governance by creating a research-based framework for CIO-led AI governance.

**Keywords:** AI Governance, CIO Leadership, Ethical AI, IT Governance, Digital Enterprise Governance

---

## i. Introduction

AI, or Artificial Intelligence, is rapidly changing how digital enterprises operate by enabling automation, improving decision-making, and enhancing operational efficiency (Najana et al., 2024). In many organisations, AI is already used across key business functions such as customer engagement, fraud detection, and operational optimisation (Desai, 2025). This trend is becoming more visible across sectors. This shift is quite noticeable in day-to-day operations (Desai, 2025). However, this rapid adoption also introduces new governance challenges, and in many cases these challenges are still evolving. These are often linked to transparency, accountability, and ethical decision-making (Al-Maamari, 2025).

Several governance frameworks, including the European Union Artificial Intelligence Act (European Union, 2024), ISO/IEC 42001 Artificial Intelligence Management Systems (ISO/IEC, 2023), and the NIST AI Risk Management Framework (NIST, 2023) provide structured approaches. However, in most cases the focus remains on organisational and technical controls. In practice, these frameworks mainly emphasise transparency, accountability, and risk management. Even so, they do not clearly define executive-level governance responsibilities. Prior IT governance research shows that executive leadership plays a direct

role in ensuring governance effectiveness and accountability (Weill & Ross, 2004), but this aspect is not strongly reflected in existing AI governance frameworks.

CIOs, as enterprise technology leaders, are responsible for governance oversight of enterprise systems, including AI. This responsibility already exists in traditional IT governance. However, there is still limited research that clearly defines CIO-specific leadership competencies required for AI governance, particularly in large enterprise environments (Weinzimer, 2023; Li et al., 2021). This gap tends to become more visible as organisations scale their AI initiatives.

## **ii. Theoretical Foundation**

This research is grounded in Upper Echelons Theory, Socio-Technical Systems Theory, and IT Governance Theory. Together, these provide the theoretical base for understanding CIO-led AI governance.

Upper Echelons Theory (Hambrick & Mason, 1984) suggests that organizational outcomes are shaped to a large extent by executive leadership characteristics, their strategic decisions, and the authority they hold. In enterprise settings, CIOs act as senior leaders responsible for technology governance, and therefore play a direct role in influencing AI governance outcomes (Gulzar, 2022). From this perspective, governance effectiveness is closely tied to CIO competencies, their decision-making role, and how governance responsibilities are exercised in practice (Li et al., 2021).

Socio-Technical Systems Theory (Trist & Bamforth, 1951), on the other hand, shifts the focus toward alignment. It emphasizes that performance depends on how well technical and social systems work together. In AI governance, this interaction becomes quite visible. Technical elements such as algorithms, data infrastructure, and automation systems operate alongside social components like leadership, governance policies, and organizational structures. If these are not aligned, governance tends to weaken. Effective AI governance therefore depends on how well these two sides are coordinated (Basir, 2025; Mäntymäki et al., 2022).

IT Governance Theory (Weill & Ross, 2004) provides a more structured view of governance itself. It explains how decision rights are defined, how accountability is assigned, and how governance mechanisms are established within organizations. In this setup, CIOs function as key governance authorities. They are responsible for compliance, risk management, and ensuring that technology initiatives remain aligned with broader enterprise objectives (Eisenberg et al., 2025). This makes the theory particularly relevant when looking at how CIO-led AI governance is implemented in practice (Basir, 2025).

Taken together, these theories offer a combined explanation. Upper Echelons Theory highlights leadership influence, Socio-Technical Systems Theory explains the interaction between systems and governance, and IT Governance Theory clarifies how authority and accountability are structured. When viewed together, they provide a more complete understanding of AI governance in digital enterprises.

At the same time, this research leans more heavily on IT Governance Theory and Socio-Technical Systems Theory. IT Governance Theory highlights the role of executive leadership in maintaining accountability, ensuring governance effectiveness, and aligning technology with business strategy (Weill & Ross, 2004).

CIOs sit at the center of this, overseeing enterprise technology and ensuring compliance requirements are met.

Socio-Technical Systems Theory further reinforces the need for alignment. Governance is not just about systems or policies in isolation. It depends on how technical systems, organizational leadership, and governance processes come together. In practical terms, AI governance requires both strong technical mechanisms and active executive oversight working in parallel.

### **iii. Problem Statement**

The rapid adoption of AI technologies has created governance challenges within digital enterprises. While governance frameworks such as ISO/IEC 42001 and NIST AI RMF provide governance guidance, they do not define executive leadership competencies required for operational AI governance. (National Institute of Standards and Technology, 2023) Organisations face governance risks due to the absence of structured executive leadership models for AI governance. (Burrell, 2025) Ethical guidelines, such as those of UNESCO (2021) and the OECD (2019), emphasise governance principles, but operational governance requires executive leadership accountability. (UNESCO, 2021) Industry research indicates that organisations struggle to operationalise AI governance due to a lack of governance leadership structures. CIOs play a central role in enterprise IT governance but lack structured models for AI governance (McKinsey, 2024; Gartner, 2025).

This research addresses the executive leadership gap by establishing the foundation for developing a CIO-centric AI governance framework.

### **iv. Research Objectives**

The objectives of this research are:

- To examine CIO leadership roles in AI governance
- To identify governance competencies required for CIO-led AI governance
- To analyse governance challenges faced by CIOs
- To develop a CIO-centric AI governance framework

### **v. Research Questions**

RQ1: What leadership competencies are required for CIO-led AI governance?

RQ2: What governance responsibilities do CIOs perform in enterprise AI governance?

RQ3: How can a CIO-centric AI governance framework be developed and empirically validated?

### **vi. Proposed Research Design**

This study adopts a sequential exploratory mixed-methods design (Creswell & Plano Clark, 2018). This approach is commonly used when qualitative insights need to be validated through quantitative analysis. In the qualitative stage, purposive sampling is used to recruit executive leaders involved in AI governance, including CIOs, CTOs, CISOs, CDOs, and Heads of IT. Semi-structured interviews are typically used to explore governance responsibilities, competencies, and leadership challenges.

The quantitative stage focuses on validating governance constructs using IT governance professionals. This includes IT managers, architects, and governance professionals involved in AI governance

implementation. The expected sample size ranges between 120–200 participants to ensure statistical validity (Hair et al., 2019).

### **vii. Proposed Conceptual Model For CIO-led AI Governance**

This research proposes a CIO-centric AI governance conceptual model grounded in Upper Echelons Theory, Socio-Technical Systems Theory, and IT Governance Theory. It positions CIO leadership competencies as central drivers that influence governance mechanisms, socio-technical alignment, and overall AI governance effectiveness (Weinzimer, 2023).

The model further draws on Upper Echelons Theory (Hambrick & Mason, 1984), Socio-Technical Systems Theory (Trist & Bamforth, 1951), and IT Governance Theory (Weill & Ross, 2004) to strengthen its theoretical base. In this context, CIO leadership competencies act as a core governance driver, shaping governance mechanisms, ethical oversight, socio-technical alignment, and enterprise AI governance effectiveness (Mäntymäki et al., 2022). Overall, the model provides both a theoretical and empirical foundation (Creswell & Plano Clark, 2018) for the development of a validated CIO-centric AI governance framework (Weinzimer, 2023).

### **viii. Expected Contribution**

This research contributes to academic and practical domains. Academically, it extends IT governance theory into the AI governance context and provides empirical insights into CIO governance leadership. In practice, it supports CIO leadership by providing structured guidance for AI governance implementation.

### **ix. Sampling Size Justification**

The qualitative phase uses purposive elite sampling to recruit senior executive leaders involved in AI governance, including CIOs, CTOs, CISOs, CDOs, and Heads of IT. These participants are selected because they represent information-rich cases with direct strategic oversight and practical exposure to governance decisions. Previous research indicates that thematic saturation is often reached within approximately 12–20 interviews (Guest, Bunce, & Johnson, 2006). However, this study follows a more flexible approach based on the concept of information power (Malterud et al., 2016). This concept suggests that when participants are highly specialised and closely aligned with the research objective, smaller sample sizes can still be sufficient.

In this context, access to C-suite professionals is naturally limited, and at the same time, elite interviews (Guest et al., 2006) are expected to provide deeper and more focused insights. Because of this, a target sample of 6–12 participants is considered methodologically appropriate for the qualitative phase.

Data collection will continue until thematic sufficiency is achieved. In practice, this refers to the stage where additional interviews contribute little or no new insights. This approach helps maintain both research rigour and practical feasibility.

Mixed-methods research guidelines also support the use of purposive sampling, particularly when selecting domain experts. This strengthens the depth and validity of qualitative findings (Creswell & Plano Clark, 2018).

For the quantitative phase, the focus shifts to validating governance competencies and framework constructs identified during the qualitative stage. The participants in this phase will include IT governance professionals who are directly involved in enterprise AI governance implementation.

To support multivariate statistical analysis, including factor analysis and regression, an adequate sample size is required. Prior studies recommend a minimum range of 100–200 respondents to ensure statistical reliability, validity, and generalizability of the findings (Hair et al., 2019). This range is therefore considered appropriate for the quantitative phase.

#### **x. Population and Sampling Scope**

This study adopts a global, role-based sampling approach, targeting executive leaders and IT governance professionals who are involved in enterprise AI governance. The qualitative phase mainly focuses on senior technology executives, including CIOs, CTOs, CISOs, CDOs, and Heads of IT. These participants are selected based on their current or previous experience in executive leadership roles within enterprise technology governance, particularly where they have contributed to AI governance decision-making processes. This role-based sampling approach is intended to ensure that participants with relevant governance expertise are included, regardless of differences in organizational size, industry sector, or geographic location. In many cases, executive leadership experience in enterprise AI governance is treated as the primary inclusion criterion, rather than factors such as organizational revenue. This helps ensure that the governance insights are driven more by leadership experience than by firm size.

The quantitative phase extends the population to include IT governance professionals who are directly involved in AI governance implementation. This includes IT Directors, IT Managers, Enterprise Architects, Information Security leaders, and other technology governance professionals. Including this broader group allows for statistical validation of governance constructs that emerge from the qualitative phase.

The research follows a global sampling scope, with participants drawn from multiple geographic regions as well as industries such as information technology, financial services, telecommunications, healthcare, and digital enterprise environments. This wider coverage improves both the generalizability and the external validity of the proposed CIO-centric AI governance framework, especially given the global nature of AI governance challenges in modern enterprises.

In addition to this, the study continues to apply a role-based sampling strategy targeting senior technology executives, including CIOs, CTOs, CISOs, CDOs, and Heads of IT. Participants are selected based on their governance leadership experience in enterprise technology and their involvement in AI-related decision-making. At the same time, the quantitative phase includes IT governance professionals who are responsible for implementing governance practices in real-world environments. Overall, this approach ensures that individuals with relevant governance expertise are represented across industries and geographic regions. It also strengthens the external validity and generalizability of the research findings. Finally, the study adopts a global, role-based sampling approach that includes CIOs, CTOs, CISOs, CDOs, Heads of IT, and IT governance professionals. Selection is based primarily on governance experience rather than organizational size or revenue, ensuring consistency in the type of expertise captured.

## xi. Conclusion

AI governance presents significant leadership challenges in digital enterprises. Existing governance frameworks provide principles but do not clearly define the executive leadership competencies required for operational governance. This research establishes a foundation for developing a CIO-centric AI governance framework using a mixed-methods approach. The qualitative phase identifies governance competencies, followed by quantitative validation. This research contributes to advancing AI governance research and practice, particularly in the context of executive leadership.

## References

- [1] P. Weill and J. W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA, USA: Harvard Business School Press, 2004.
- [2] P. Weinzimer, *Strategic IT Governance 2.0: How CIOs Succeed at Digital Innovation*. New York, NY, USA: Routledge, 2023.
- [3] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research*, 3rd ed. Thousand Oaks, CA, USA: Sage Publications, 2018.
- [4] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 8th ed. Boston, MA, USA: Cengage Learning, 2019.
- [5] J. Li, M. Li, X. Wang, and J. B. Thatcher, "Strategic directions for AI: The role of CIOs and boards of directors," *MIS Quarterly*. [Online]. Available: <https://doi.org/10.25300/misq/2021/16523>
- [6] M. Najana, S. Bhattacharya, C. Kewalramani, and D. K. Pandiya, "AI and organizational transformation: Navigating the future," *IJGIS*. [Online]. Available: <https://doi.org/10.21428/e90189c8.03fab010>
- [7] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? An experiment with data saturation and variability," *Field Methods*, vol. 18, no. 1, pp. 59–82, 2006.
- [8] K. Malterud, V. D. Siersma, and A. D. Guassora, "Sample size in qualitative interview studies: Guided by information power," *Qualitative Health Research*, vol. 26, no. 13, pp. 1753–1760, 2016.
- [9] European Union, "Regulation (EU) 2024/1689 (Artificial Intelligence Act)," Brussels, Belgium, 2024.
- [10] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD, USA: NIST, 2023.
- [11] International Organization for Standardization, *ISO/IEC 42001:2023 Artificial Intelligence Management System*. Geneva, Switzerland: ISO, 2023.
- [12] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*. Paris, France, 2021.
- [13] Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence*. Paris, France, 2019.
- [14] National Institute of Standards and Technology, "NIST AI RMF to ISO/IEC 42001 crosswalk." [Online]. Available: [https://airc.nist.gov/docs/NIST\\_AI\\_RMF\\_to\\_ISO\\_IEC\\_42001\\_Crosswalk.pdf](https://airc.nist.gov/docs/NIST_AI_RMF_to_ISO_IEC_42001_Crosswalk.pdf)
- [15] M. Mäntymäki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Putting AI ethics into practice: The hourglass model," *arXiv*. [Online]. Available: <https://doi.org/10.48550/arXiv.2206.00335>
- [16] A. Al-Maamari, "AI risk management frameworks across regions," *arXiv*. [Online]. Available: <https://doi.org/10.48550/arXiv.2503.05773>

- [17] I. W. Eisenberg, L. Gamboa, and E. Sherman, "Unified control framework for AI governance," \*arXiv\*. [Online]. Available: <https://doi.org/10.48550/arXiv.2503.05937>
- [18] O. A. Basir, "Social responsibility stack for AI governance," \*arXiv\*. [Online]. Available: <https://doi.org/10.48550/arXiv.2512.16873>
- [19] R. Gulzar, "CIO guide to IT governance policy framework," Gartner Research, 2022.
- [20] D. Desai, "AI innovation vs security in enterprises," \*Help Net Security\*, Mar. 24, 2025. [Online]. Available: <https://www.helpnetsecurity.com/2025/03/24/ai-ml-tool-enterprise-usage/>
- [21] S. Burrell, "AI governance risks in organizations," \*ITPro\*, Jul. 24, 2025. [Online]. Available: <https://www.itpro.com/technology/artificial-intelligence/organizations-face-ticking-timebomb-over-ai-governance>
- [22] McKinsey & Company, \*Scaling Responsible AI: From Principles to Practice\*. New York, NY, USA: McKinsey Global Institute, 2024.
- [23] Gartner, \*Top Strategic Technology Trends for 2025: Responsible and Trustworthy AI\*. Stamford, CT, USA: Gartner Research, 2025.