International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, Delaware, USA
Volume 13– No. 3, June 2026 – www.ijais.org

Racing Ahead, Governing Behind: An Institutional Analysis of AI Governance Readiness in Global Capability Centers

Chandrasekar Umapathy
Indian Institute of Management Sambalpur, Odisha, India
University of Bordeaux, Bordeaux, France

ABSTRACT

The proliferation of artificial intelligence (AI) in Global Capability Centres (GCCs) has created a critical governance readiness gap. This paper presents an in-depth field study examining AI governance configurations in GCC environments, the institutional and efficiency factors that determine governance readiness, and pathways through which organisations develop more rigorous governance over time. Drawing on the constrained-efficiency framework [1] — which integrates transaction cost theory [2, 3] and institutional theory [4, 5] — the study analyses empirical evidence from 28 semi-structured interviews across five GCC organisations. Applying the Gioia et al. [6] qualitative methodology, four types of AI governance readiness are identified: incipient, ostensible, implicit, and explicit. Five theoretical propositions are derived and assessed, addressing coercive institutional forces, efficiency motives, innovation-governance velocity asymmetry, agentic AI framework limitations, and the engagement gap at executive and board levels. The NIST AI RMF 1.0 [7] is applied as a governance maturity diagnostic, revealing that participating GCCs score at Level 1 on Govern and Map functions against a sector average of Level 2 to 3 [8]. A readiness pathway model illustrates how governance configurations evolve under competing institutional and efficiency pressures.

General Terms

AI Risk Management, Governance Frameworks, Institutional Theory, Emerging Markets, Cybersecurity, Information Systems.

Keywords

AI governance; Global Capability Centres; NIST AI RMF; agentic AI; shadow AI; institutional isomorphism; constrained-efficiency framework; DPDPA 2023; cybersecurity governance.

1. INTRODUCTION

Artificial intelligence (AI) risks constitute among the most consequential technology governance challenges confronting organisations in the digital economy [9]. Despite sustained growth in AI investment across industries [10], governance infrastructure has consistently lagged AI deployment velocity. Generative AI tools, large language model (LLM) applications, and agentic AI systems — capable of autonomous multi-step task execution — have transformed AI from a discretionary investment into a baseline operational capability [11], frequently without corresponding governance development.

Global Capability Centres have evolved from cost-arbitrage vehicles into primary sites of technology innovation, advanced analytics, and AI development for multinational corporations. India alone hosts more than 1,700 GCCs employing upward of 1.9 million technology professionals [8]. GCC AI governance presents a structurally complex challenge: these organisations must simultaneously satisfy the risk frameworks of a multinational parent organisation, the regulatory obligations of the host country, and the norms of an AI tool ecosystem whose terms of service are frequently misaligned with enterprise data governance requirements [12].

AI governance, as defined by the National Institute of Standards and Technology [7] and ISO/IEC 42001:2023 [13], addresses how organisations establish policies, accountability structures, risk controls, and oversight mechanisms for the responsible development, deployment, and monitoring of AI systems. Despite sustained growth in AI investment, governance practices in GCCs are materially underdeveloped: fewer than one in three Indian GCCs has a formally documented AI governance policy, and fewer than 15 percent have dedicated AI governance personnel [8].

A particular governance challenge arises from agentic AI systems capable of executing multi-step tasks autonomously. Such systems introduce governance challenges qualitatively beyond those of conventional AI/ML output generation [14], because they act before human review is possible. The OWASP Top 10 for LLM Applications [14] identifies excessive agency and insecure tool use as among the most critical AI risks.

There is limited research evidence about which AI governance structures GCCs adopt in practice, how governance actors collaborate, and which factors affect configuration choices. The present study addresses this gap by drawing on the constrained-efficiency framework [1], which integrates transaction cost theory [2, 3] and institutional theory [4, 5]. In the IS governance literature, prior research has examined individual governance actors or frameworks [15, 16] but has not examined the combined functioning of AI governance across the full principal hierarchy in GCC environments.

The paper addresses three research questions: (RQ1) What AI governance configurations exist in GCC environments vis-à-vis governance readiness? (RQ2) Why does AI governance readiness matter in GCC environments? (RQ3) Which institutional and efficiency factors shape AI governance development pathways? Three specific contributions are made. First, a two-dimensional AI governance readiness framework is developed identifying four readiness types — incipient, ostensible, implicit, and explicit. Second, five theoretical propositions are derived and empirically assessed using the constrained-efficiency framework [1], applied for the first time to GCC AI governance. Third, a readiness pathway model

illustrates how governance configurations evolve under competing institutional and efficiency pressures.

2. LITERATURE REVIEW

2.1 AI governance in GCC environments

AI governance encompasses the accountability structures, policies, and processes through which organisations exercise strategic direction and oversight of AI risk management [7]. The NIST AI RMF 1.0 [7] organises AI governance across four functions: Govern (policies, accountability, risk culture), Map (asset inventory, risk context, taxonomy), Measure (controls, monitoring, metrics), and Manage (incident response, remediation, improvement). Prior IS governance research distinguishes between governance structures and relational mechanisms [17], addressing respectively who holds what role and how collaboration and monitoring occur across governance levels [21].

In GCC environments, the AI governance principal hierarchy comprises five levels: AI developers and technical operations (first); AI risk management and compliance — covering India's Digital Personal Data Protection Act 2023 [20] and CERT-In Directions 2022 [19] — (second); internal governance assurance (third); GCC operational leadership and parent executive management (fourth); and parent board of directors (fifth). AI governance research has principally examined individual actors in isolation [15, 22], without examining the combined functioning of AI governance across the full principal hierarchy in GCC environments [16]. The SEC cybersecurity disclosure rules [23] and international regulatory convergence further amplify the need for integrated multi-level governance in GCC contexts. Evidence suggests GCC AI governance is materially underdeveloped, with zero percent AI asset inventory coverage reported in the average Indian GCC [8].

Table 1 maps prior IS governance literature against the dimensions of this study, demonstrating the research gap this paper addresses.

Table 1. Prior IS governance literature — positioning of the present study

Study	Focus	Theory	Method	Gap vis-à-vis this study
Slapnicar et al. [16]	Cybersecurity governance; 5LoA	Constrained -efficiency	Field study	Not AI-specific; not GCC
Wilkin & Chenhall [15]	IT governance reflections	IT governance	Lit. review	Not AI; not GCC
Steinbart et al. [22]	IS audit collaboration	Agency theory	Survey	Single level; not GCC
Ogbanufe et al. [29]	IS commitment pressures	Institutional theory	Survey	US only; not GCC
NASSCOM [8]	GCC AI maturity	Benchmarki ng	Survey	No theoretical model
This study	AI governance readiness across principal hierarchy	Constrained -efficiency; institutional theory	Field study (5 GCCs, 28 interview s)	Multi-sector Indian GCCs; AI-specific; multi-jurisdictional

2.2 Efficiency/effectiveness and institutional determinants

The constrained-efficiency framework [1] integrates two complementary theories. Transaction cost theory [2, 3, 24] contends that organisations implement governance structures that economise on organisational costs, optimising performance within institutional constraints. A common criticism is that transaction cost theory is undersocialised — taking almost no account of the social or institutional context in which organisations operate [27, 1]. Institutional theory [4, 5] suggests that governance decisions draw on taken-for-granted approaches or those most acceptable within an organisational field. Adopting a recognised governance model can become a means of legitimising an organisation's approach [25], and in conditions of uncertainty this need may be fundamental to governance configuration choices. Roberts and Greenwood [1] consider these theories complementary: organisations optimise efficiency and effectiveness given institutional pressures. Gordon et al. [28] demonstrate that enterprise risk management positively affects firm performance when well fitted to organisational characteristics, a finding that extends to GCC AI governance contexts.

Three institutional forces shape GCC AI governance. Coercive forces — laws, regulations, and parent mandates [26] — represent baseline compliance requirements. In GCC environments, coercive pressures operate at two levels simultaneously: parent-organisation enterprise standards calibrated to home-country regulatory environments, and host-country obligations including DPDPA 2023 [20] and CERT-In Directions 2022 [19]. Normative forces arise through professional certifications and networks [4], influencing which AI risk approaches professionals consider legitimate [29]. Mimetic forces arise when organisations imitate successful peers — particularly strong under high uncertainty [8]. The enterprise risk management and COSO frameworks [42] provide additional normative standards that GCCs increasingly adopt. The conceptual framework (Figure 1) guides the research design and five theoretical propositions developed from empirical evidence in Section 4.

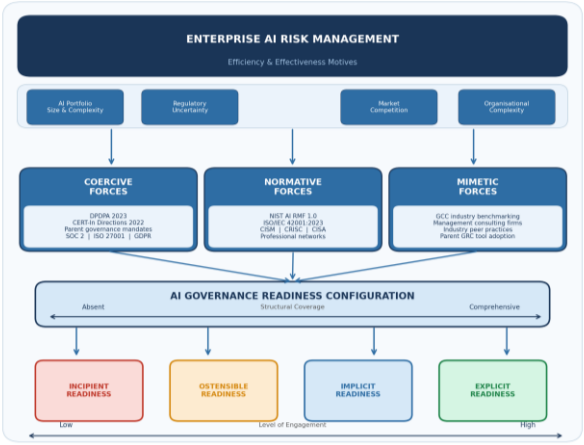

Fig. 1. Conceptual framework of AI governance readiness in GCC environments

3. METHOD

3.1 Research design and epistemological position

The research aim requires access to subjective meanings, organisational practices, and institutional pressures that quantitative methods cannot adequately capture. Accordingly, a constructivist epistemological position is adopted [30, 31], treating AI governance readiness as a socially constructed phenomenon best understood through the accounts of those whose roles enact it. An in-depth field study design is employed following Eisenhardt [32], particularly appropriate when the phenomenon is complex, under-theorised, and embedded in its organisational and institutional context [38]. The multi-site design — five GCC organisations with theoretically contrasting institutional and efficiency contexts — follows Eisenhardt and Graebner [33], enabling pattern matching across cases.

A total of 28 semi-structured interviews were conducted across five GCC organisations between January and May 2025. Semi-structured interviewing was selected to allow consistent coverage of the conceptual framework dimensions whilst permitting respondents to raise unanticipated considerations [34]. Protocols were developed for each governance level. Purposeful sampling [35] targeted individuals in positions critical to AI governance and risk management. Sampling continued until theoretical saturation was reached [36, 37] — no new first-order codes emerged after interview 22; the final six interviews confirmed code stability across all five organisations.

3.2 Participating organisations

Five GCC organisations with materially different AI portfolio compositions, regulatory exposure profiles, and parent governance structures were recruited to maximise theoretical variation and support pattern-matching analysis [32]. Four are Indian GCC subsidiaries of US-headquartered multinational corporations; the fifth operates within a regulated financial services environment. Table 2 provides a summary.

Table 2. Participating GCC organisations

Org.	Sector	Location	AI Portfolio	N	Regulatory Exposure
GCC-A	Technology services	Bengaluru	Production LLM + agentic	7	DPDPA; CERT-In; US frameworks
GCC-B	Healthcare analytics	Bengaluru	Analytics + GenAI pilots	5	DPDPA; CERT-In; HIPAA
GCC-C	Professional services	Hyderabad	Production LLM + analytics	8	DPDPA; CERT-In; GDPR
GCC-D	Financial technology	Pune	Agentic AI (prototype)	3	DPDPA; CERT-In; US frameworks
GCC-E	Regulated fin. services	Bengaluru	Production AI + regulated	5	DPDPA; CERT-In; GDPR; prudential
Total	—	India	—	28	—

3.3 Data collection

Data were collected through multiple sources consistent with Yin's [38] triangulation principle: 28 semi-structured interviews (Table 3), documentary analysis of internal governance materials (AI governance policy documents, UEBA alert records, internal audit reports, regulatory compliance self-assessments), and NASSCOM [8] and Gartner [11] sector benchmarking data as secondary sources.

Table 3. Interview data collection summary

Codes	GCC	N	Period	Duration	Mode	Levels
A1-A7	GCC-A	7	Jan-Feb 2025	55-70 min	Recorded	All five
B1-B5	GCC-B	5	Feb 2025	50-65 min	Recorded	Levels 1-4
C1-C8	GCC-C	8	Feb-Mar 2025	55-75 min	Rec.+notes	All five
D1-D3	GCC-D	3	Mar 2025	45-60 min	Field notes	Levels 1-2, exec.
E1-E5	GCC-E	5	Apr 2025	60-80 min	Recorded	All five
Total	—	28	Jan-Apr 2025	~1,700 min	—	—

3.4 Data analysis and quality criteria

Analysis proceeded in two stages following Gioia et al. [6]. In the first stage, each transcript was coded in line with the conceptual framework (Fig. 1) and open coding applied [41]. First-order concepts were progressively abstracted to second-order concepts and aggregate dimensions, producing a rigorous data structure. In total, 63 first-order concept codes and 21 second-order concepts were identified, aggregating to seven dimensions (Appendix B). In the second stage, pattern-matching and explanation-building across cases [38, 39] were used to develop the readiness typology and derive the pathway model.

Four quality criteria were applied following Yin [38]. Construct validity was addressed through multiple data sources, member checking of all transcripts within two weeks, and explicit framework specification prior to data collection. Internal validity was addressed through explanation-building, pattern-matching, and systematic pursuit of disconfirming evidence. External validity was addressed through deliberate multi-site design across five organisations. Reliability was addressed through a documented interview protocol, structured Gioia coding [6], and a transparent audit trail from raw data to theoretical constructs [40]. No respondent challenged the overall characterisation of their organisation's governance posture during member checking.

4. FINDINGS AND THEORETICAL PROPOSITIONS

4.1 AI governance configurations vis-à-vis readiness

4.1.1 AI governance structures

First and second governance levels. Across all five participating GCCs, the first governance level (AI developers) and the second governance level (AI risk management and compliance) were consistently blended without formal structural segregation. This blending was observed regardless of organisational size, AI portfolio complexity, or regulatory exposure.

A recurring and analytically significant observation was the strategic sensitivity of AI training datasets — particularly those underpinning production LLM-based knowledge work automation systems — combined with access control frameworks that had not been updated to reflect this sensitivity. In GCC-A and GCC-C, training datasets represented decades of accumulated institutional knowledge. Despite this strategic significance, access governance frameworks remained calibrated to general data handling rather than AI-specific risk:

> *"Our data team and the AI engineers effectively operate as one function. The risk oversight is there in principle. In practice the same people who build the models manage the training data." — GCC-A Head of AI Development*

The second governance level also played an important role in determining reporting metrics for executive management. However, across all participating GCCs, maturity around AI-specific key risk indicators (KRIs) was consistently low. Coercive regulatory forces — particularly India's DPDPA 2023 — were cited as an emerging driver of governance restructuring:

> *"DPDPA has changed the conversation at board level. Questions are now asked about data flows that were not asked before. The challenge is that the approved tool list was built before DPDPA and has not been reviewed against it." — GCC-C Head of AI Risk*

Third governance level. Internal governance assurance was not considered critically involved in AI risk management across four of the five participating GCCs — consistent with prior IS audit research showing internal audit functions focus predominantly on reviewing compliance with existing policies [43, 44]. The exception was GCC-E, where the internal audit function had developed AI-specific capability:

> *"AI is covered as part of the general IT audit scope, but no separate AI audit programme exists. Specialist AI assessment relies heavily on external providers." — GCC-B Internal Audit Manager*

A structural challenge was the pace of AI system development relative to audit cycle timelines. In most participating GCCs, AI systems moved from prototype to production within timeframes shorter than internal audit cycles — in some cases three to four years between governance reviews. Fourth and fifth governance levels. AI governance reporting was bottom-up driven in all cases:

> *"Technical AI risk has to be translated into something the executive committee can act on. A dashboard is provided — red, amber, green — but half the time it is unclear whether the reds are understood." — GCC-D CISO*

The contrast observed in GCC-E is analytically significant: the parent organisation's Chief Risk Officer had collaborated with the GCC Managing Director to develop AI-specific risk appetite statements and KRIs — the only instance where upper governance levels actively shaped governance instruments. This mirrors the formal/real authority distinction [18]: formal authority rests with boards, but real authority over AI governance decisions rests with technical specialists:

> *"The Board ensures management has an appropriate AI risk framework and sufficient resources. Beyond that, the CISO and the AI team are entirely relied upon." — GCC-A Audit Committee Chair*

4.1.2 Governance relational mechanisms

Intense collaboration between AI developers (first level) and AI risk management (second level) was described across all participating GCCs. However, this collaboration did not extend consistently to the third governance level:

> *"Risk management conducts a risk assessment and then internal audit conducts its own assessment. There is no shared framework, so two different maturity ratings are produced for the same system." — GCC-C IT Audit Lead*

Such disconnection contributed to fragmented governance reporting, no integration into the parent's enterprise risk management framework, and escalation driven by the individual judgement of the CISO rather than by defined process. The significant information asymmetry between technical governance roles and upper-level principals placed a disproportionate governance dependency on a single individual in each GCC.

4.1.3 Defining AI governance readiness types

AI governance readiness is conceptualised according to two dimensions: (1) structural governance coverage — ranging from absent to comprehensive; and (2) the level of active engagement of governance actors — ranging from low to high.

Figure 2 presents the four readiness types. Incipient readiness: limited structure, low engagement. Ostensible readiness: formal governance exists but engagement is low. Implicit readiness: limited formal structure but high active engagement. Explicit readiness: comprehensive governance with active engagement at all levels.

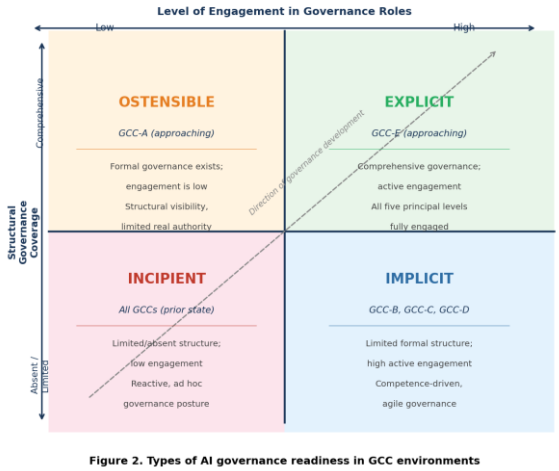

Figure 2. Types of AI governance readiness in GCC environments

Fig. 2. Types of AI governance readiness in GCC environments

4.2 NIST AI RMF governance maturity assessment

The NIST AI RMF 1.0 [7] is applied as a governance maturity diagnostic across all four functions. Maturity levels were assessed through a structured protocol applied to each interview, cross-referenced with documentary evidence. Each function was rated on a five-point scale: Level 1 (Initial — ad hoc, reactive), Level 2 (Developing — some awareness and informal processes), Level 3 (Defined — documented policies), Level 4 (Managed — monitored and measured), and Level 5 (Optimising — continuous improvement). Ratings were determined through triangulation of interview responses, documentary evidence (audit reports, policy documents, compliance self-assessments), and cross-comparison with NASSCOM [8] sector benchmarks. Figure 3 presents the maturity assessment results.

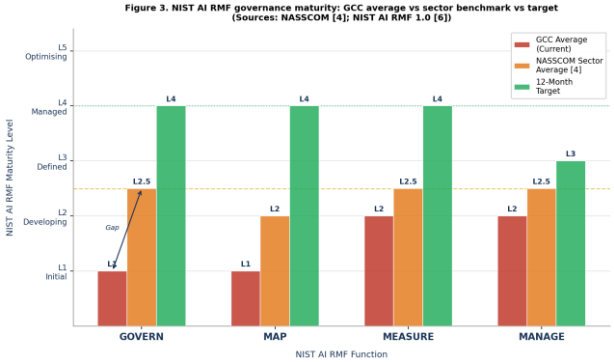

Fig. 3. NIST AI RMF governance maturity: GCC average vs sector benchmark [8] vs 12-month target. Ratings based on triangulated evidence from 28 interviews, documentary analysis, and NASSCOM sector benchmarks. (L1=Initial; L2=Developing; L3=Defined; L4=Managed; L5=Optimising)

Three findings from Figure 3 are analytically significant. First, Govern and Map functions are at Level 1 across most participating GCCs — below the sector average [8], which itself represents a materially inadequate governance posture relative to the complexity of AI portfolios deployed. All five GCCs were rated Level 1 on Govern because none had documented AI risk appetite statements, formal AI governance committee structures, or AI-specific accountability frameworks in place. Map was rated Level 1 universally because no participating GCC maintained a comprehensive AI asset inventory — confirming NASSCOM's [8] finding of zero percent AI asset inventory coverage. Second, the Measure function's Level 2 rating is attributable primarily to UEBA platform deployments mandated by parent organisations rather than organically developed governance controls. Third, the gap between current maturity and proposed twelve-month targets requires structural change.

Table 4. Governance gap indicators — participating GCCs vs NASSCOM sector average [8]

Governance Gap Indicator	Sector Avg [8]	GCC-A	GCC-C	GCC-E
AI asset inventory coverage	34%	0%	0%	22%
AI-specific policy documentation	Basic	None	Partial	Comprehensive
Agentic AI governance policy	12%	None	None	None
AI incident response playbook	29%	None	None	Partial
Dedicated AI governance FTEs	1.2	0	0	1
AI risk training (% staff trained)	38%	~15%	~20%	~45%
Multi-jurisdictional compliance map	46%	None	Partial	Partial

4.3 Five structural antecedents: evidence and propositions

4.3.1 Innovation-governance velocity asymmetry

A systematic asymmetry was observed across all five participating GCCs between the pace of AI capability development and the pace of governance infrastructure development. GCC-A deployed a production LLM system, established an agentic AI programme, and extended its cloud analytics platform between 2023 and early 2025 — without updating access control policies, vendor management frameworks, or incident response procedures. An internal IT audit in August 2024 identified more than 30 unsanctioned AI tools in active use, with proprietary work product submitted to third-party tools whose terms of service permitted use of inputs for model training [12]. This asymmetry is structural rather than discretionary, consistent with the constrained-efficiency framework's [1] prediction that efficiency motives will systematically outpace governance investment absent explicit coupling mechanisms:

> *"When the AI governance policy was established, agentic AI was not in scope. Eighteen months later, a team is building agentic systems and the policy has no provisions for them — no authorisation boundaries, no action logging requirements." — GCC-A CISO*

> *Proposition 1 (P1): In GCC environments characterised by aggressive AI adoption mandates, governance infrastructure development will systematically lag AI capability development unless governance investment is formally indexed to AI portfolio expansion through an explicit governance-velocity coupling mechanism.*

4.3.2 Multi-principal governance misalignment

All five participating GCCs operated under three principals with partially incompatible governance expectations: parent organisations, Indian regulatory authorities (CERT-In [19] and DPDPA enforcement [20]), and GCC operational leadership. These governance vectors were not reconciled in any formal governance instrument, producing compliance gaps that no individual principal's framework could close unilaterally. This is consistent with agency-theoretic predictions [18] that information asymmetry will produce governance gaps when delivery incentives are not counterbalanced by explicit governance performance signals:

> *"Forty-seven AI tools are on the approved list. When legal was asked how many had been reviewed against DPDPA, the answer was: none." — GCC-C Head of AI Risk*

> *Proposition 2 (P2): In multi-principal GCC governance environments, AI governance inadequacy will disproportionately arise at the intersection of principal governance expectations — where no single principal's framework provides sufficient coverage.*

4.3.3 Unsanctioned AI tool adoption

Unsanctioned AI tool adoption was documented across all five participating GCCs [12]. The structural driver is procurement-process friction: formal AI tool approval timelines, calibrated for enterprise software procurement cycles, are structurally incompatible with the pace at which AI tools emerge. Governance design that reduces the relative cost of compliant behaviour will achieve better outcomes than designs that increase penalties without reducing procurement friction.

> *Proposition 3 (P3): Unsanctioned AI tool adoption in GCC environments is primarily an antecedent of governance design — specifically, procurement-process friction — rather than an antecedent of organisational culture.*

4.3.4 Agentic AI governance framework limitations

Agentic AI prototypes were being developed in three participating GCCs (GCC-A, GCC-C, GCC-D) under governance frameworks designed for conventional AI/ML output generation. No participating GCC had formal governance instruments — authorisation boundaries, mandatory action logging, human-in-the-loop mandates — designed for agentic AI. The OWASP Top 10 for LLM Applications [14] identifies excessive agency, insecure tool use, and supply chain vulnerabilities as among the most critical LLM risks. The NIST AI RMF's post-output review assumption [7] is structurally inadequate for systems that act before review is possible.

> *Proposition 4 (P4): Conventional AI governance frameworks — including the NIST AI RMF [7] — are structurally limited in governing agentic AI systems because they are premised on a post-output human review assumption that is invalidated by the pre-review autonomous action capability defining agentic systems.*

4.3.5 Engagement gap and multi-jurisdictional complexity

All five participating GCCs faced regulatory exposure spanning DPDPA 2023 [20], CERT-In Directions 2022 [19], and parent-country frameworks; three also faced extraterritorial GDPR. Parent board engagement was consistently characterised by passive report receipt, limited challenge, and disproportionate dependence on a single technical expert. The engagement gap mirrors findings from cybersecurity governance research [16] and the formal/real authority distinction [18]. Multi-jurisdictional complexity amplifies the gap: boards cannot meaningfully challenge governance reporting on DPDPA compliance or CERT-In obligations without AI-specific legal and technical literacy.

> *Proposition 5 (P5): Active engagement of executive management and parent board in AI governance will be low across GCC environments irrespective of structural coverage, reflecting information asymmetry, limited AI literacy at upper governance levels, and the bottom-up reporting dynamic.*

5. DISCUSSION

5.1 Assessment of propositions against empirical evidence

The empirical evidence provides support for all five a priori propositions. Table 5 summarises the proposition assessment.

Table 5. Proposition assessment summary

P	Focus	Assessment	Key evidential basis
P 1	Governance-velocity asymmetry	Supported — all 5	30+ unsanctioned tools; agentic AI developed without governance update
P 2	Multi-principal misalignment	Supported — all 5	DPDPA not reviewed against approved tools in any participating GCC
P 3	Unsanctioned AI — design issue	Supported — all 5	Procurement friction confirmed as primary driver across all five GCCs
P 4	Agentic AI framework limitation	Supported — all 5	No agentic governance instruments in any organisation; NIST AI RMF inadequate
P 5	Engagement gap	Supported — all 5	Passive board receipt universal; real authority concentrated in single CISO

P1 (governance-velocity asymmetry) is supported consistently across all five organisations irrespective of AI portfolio size or sector. The finding that agentic AI was being developed without triggering governance policy review in all three relevant GCCs demonstrates a systemic governance design gap. P2 (multi-principal misalignment) is confirmed: no participating GCC had reviewed its approved AI tool list against DPDPA 2023 requirements, despite the regulation having been in force since August 2023.

P4 (agentic AI framework limitation) is confirmed universally and represents the most urgent practical finding. No existing framework, including the NIST AI RMF [7], provides the upstream authorisation boundary specification and mandatory action logging required for agentic AI governance. P5 (engagement gap) is strongly and consistently supported. The pattern of passive board engagement was observed across all five GCCs without exception, mirroring findings from cybersecurity governance research [16, 44] and the cybersecurity audit literature [45].

5.2 Readiness pathway model

A key insight is that AI governance readiness in GCCs is both evolving and fluid. Figure 4 presents the readiness pathway model, illustrating how governance configurations evolve over time under competing institutional and efficiency pressures.

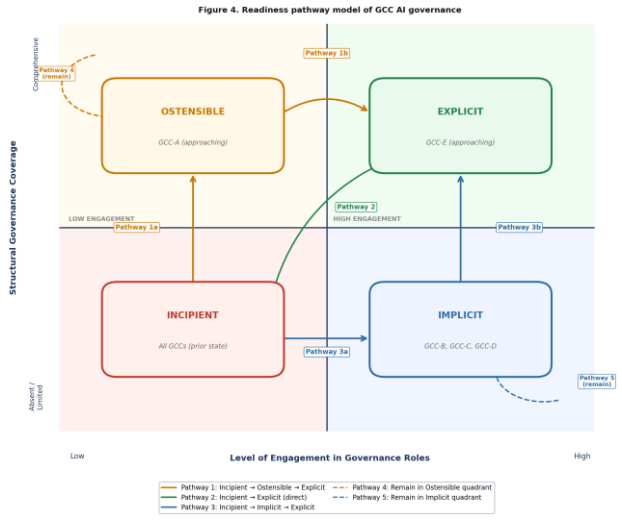

Fig. 4. Readiness pathway model of GCC AI governance

Three primary pathways are identified. Pathway 1 moves from incipient through ostensible to explicit readiness: taken when institutional forces predominate, driving structural adoption before engagement catches up (exemplified by GCC-E). Pathway 2 moves directly from incipient to explicit readiness: taken when both coercive forces and high AI risk exposure simultaneously motivate structural development and active engagement. Pathway 3 moves from incipient through implicit to explicit readiness: taken when efficiency motives are emphasised (exemplified by GCC-B and GCC-C). Pathways 4 and 5 represent quadrant-stable configurations where organisations remain in ostensible or implicit readiness absent a triggering institutional or efficiency event.

5.3 Theoretical contributions

The present study makes three theoretical contributions. First, it extends the constrained-efficiency framework [1] — previously applied to cybersecurity governance [16] — to GCC AI governance for the first time, demonstrating that GCCs experience regulatory isomorphic tension: coercive pressures from parent organisations and host-country regulators pull governance design in partially incompatible directions. Second, the study demonstrates that the engagement gap documented for cybersecurity governance [16, 44] replicates systematically in AI governance in GCC environments and is amplified by multi-jurisdictional regulatory complexity. This confirms the formal/real authority distinction [18] across technology governance domains. Third, the study provides the first empirical documentation of agentic AI governance limitations in a GCC field study setting, identifying the temporal governance gap as a framework-level limitation. This extends and operationalises the OWASP agentic AI risk taxonomy [14] in a concrete multi-principal GCC context.

5.4 Practical implications, limitations, and future research

For GCC IS governance leaders, the five structural antecedents constitute a prospective readiness diagnostic applicable before governance incidents occur. For parent organisation boards, the study demonstrates that uniform enterprise governance standards transferred without adaptation for host-country regulatory environments will reliably produce the readiness gaps documented. For regulators, the multi-jurisdictional complexity documented in P5 argues for coordinated guidance between DPDPA enforcement, CERT-In [19], and international regulatory counterparts. The SEC's approach to cybersecurity governance disclosure [23] provides a useful model for regulators seeking to mandate board-level AI governance engagement.

Three principal limitations bound this study. First, as a multi-site field study, analytical generalisation is to theoretical propositions rather than statistical populations [38]; the five propositions require quantitative testing across larger GCC samples. Second, the cross-sectional design captures configurations at a single point in time. Third, India's DPDPA 2023 enforcement guidance continues to evolve. Future research directions include longitudinal study of GCC governance configurations, quantitative survey research testing P1-P5, comparative study across GCC geographies, and dedicated empirical study of agentic AI governance design requirements.

6. CONCLUSION

AI governance configurations in GCCs and the relationships between governance levels across different organisational and institutional contexts have received scant attention in academic research. The present study addresses this gap through an in-depth field study of 28 interviews across five GCC organisations, applying the constrained-efficiency framework [1], NIST AI RMF 1.0 [7], and Gioia et al. [6] qualitative methodology.

The study develops a two-dimensional AI governance readiness framework identifying four readiness types — incipient, ostensible, implicit, and explicit — defined by structural governance coverage and active engagement of governance actors. A readiness pathway model illustrates how GCC AI governance configurations evolve under the interplay of coercive, mimetic, and normative institutional forces. Five theoretical propositions are derived and empirically assessed; all five receive empirical support across the full sample.

The most urgent practical contribution is the identification of agentic AI as a governance frontier for which existing frameworks — including the NIST AI RMF in its current form [7] — are structurally limited. The NASSCOM [8] sector benchmarks confirming zero percent AI asset inventory coverage and twelve percent agentic AI governance policy adoption establish that the governance readiness gaps documented are representative of sector-wide structural conditions. Organisations that develop AI governance infrastructure commensurately with their AI capabilities — as a proactive strategic investment — will be best positioned to realise the full value of their AI portfolios responsibly.

7. ACKNOWLEDGMENTS

The authors thank all interview respondents across the five participating GCC organisations for their time and candour. Written approval for the research was provided by the respective parent management organisations. Ethical clearance was obtained from the authors' university. The research was conducted independently without external funding.

8. REFERENCES

[1] Roberts, P.W. and Greenwood, R. (1997). Integrating transaction cost and institutional theories: Toward a constrained-efficiency framework for understanding organizational design adoption. Academy of Management Review, 22(2), 346-373.

[2] Coase, R.H. (1937). The nature of the firm. Economica, 4(16), 386-405.

[3] Williamson, O. (1975). Markets and Hierarchies. Free Press, New York.

[4] DiMaggio, P.J. and Powell, W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147-160.

[5] Lawrence, T.B. and Shadnam, M. (2008). Institutional theory. The International Encyclopedia of Communication.

[6] Gioia, D.A., Corley, K.G. and Hamilton, A.L. (2013). Seeking qualitative rigor in inductive research. Organizational Research Methods, 16, 15-31.

[7] National Institute of Standards and Technology (2023). AI Risk Management Framework (AI RMF 1.0). NIST AI 100-1.

[8] NASSCOM (2024). GCC State of the Industry Report 2024. NASSCOM, New Delhi.

[9] World Economic Forum (2023). Global Risk Report 2023. World Economic Forum, Geneva.

[10] McKinsey and Company (2023). The State of AI in 2023: Generative AI's Breakout Year. McKinsey Global Institute.

[11] Gartner (2024). Top Strategic Technology Trends for 2024: Agentic AI. Gartner Research Note G00796823.

[12] Cyberhaven (2023). The AI Data Exposure Report. Cyberhaven Research, Palo Alto, CA.

[13] ISO/IEC 42001:2023. Artificial Intelligence — Management System Standard. International Organization for Standardization.

[14] OWASP (2024). Top 10 for Large Language Model Applications (Version 2.0). Open Web Application Security Project.

[15] Wilkin, C.L. and Chenhall, R.H. (2020). Information technology governance: Reflections on the past and future directions. Journal of Information Systems, 34(2), 257-292.

[16] Slapnicar, S., Axelsen, M., Bongiovanni, I. and Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. International Journal of Accounting Information Systems, 51, 100642.

[17] Van Grembergen, W., De Haes, S. and Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. In: Van Grembergen, W. (Ed.), Strategies for Information Technology Governance. IGI Global, pp. 1-36.

[18] Aghion, P. and Tirole, J. (1997). Formal and real authority in organizations. Journal of Political Economy, 105(1), 1-29.

[19] CERT-In (2022). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000. Ministry of Electronics and Information Technology, Government of India.

[20] Ministry of Law and Justice, Government of India (2023). The Digital Personal Data Protection Act, 2023. Gazette of India, Extraordinary.

[21] De Haes, S. and Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. Information Systems Management, 26(2), 123-137.

[22] Steinbart, P.J., Raschke, R.L., Gal, G. and Dilla, W.N. (2018). The influence of a good relationship between the internal audit and information security functions on

information security outcomes. Accounting, Organizations and Society, 71, 15-29.

[23] Securities and Exchange Commission (2022). Cybersecurity risk management, strategy, governance, and incident disclosure. March.

[24] Williamson, O.E. (2007). Transaction cost economics: An introduction. Economics Discussion Paper No. 2007-3.

[25] Power, M. (2009). The risk management of nothing. Accounting, Organizations and Society, 34, 849-855.

[26] Burdon, W.M. and Sorour, M.K. (2020). Institutional theory and evolution of 'a legitimate' compliance culture. Journal of Business Ethics, 162(1), 47-80.

[27] Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. American Journal of Sociology, 91, 481-510.

[28] Gordon, L.A., Loeb, M.P. and Tseng, C.Y. (2009). Enterprise risk management and firm performance: A contingency perspective. Journal of Accounting and Public Policy, 28(4), 301-327.

[29] Ogbanufe, O., Kim, D.J. and Jones, M.C. (2021). Informing cybersecurity strategic commitment through top management perceptions. Information and Management, 58(7), 103507.

[30] Lincoln, Y.S., Lynham, S.A. and Guba, E.G. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. In: Denzin, N.K. and Lincoln, Y.S. (Eds.), The Sage Handbook of Qualitative Research, 4th ed. Sage Publications, pp. 97-128.

[31] Constantino, T.E. (2008). The SAGE Encyclopedia of Qualitative Research Methods. SAGE Publications, Thousand Oaks, CA.

[32] Eisenhardt, K.M. (1989). Building theories from case study research. Academy of Management Review, 14(4), 532-550.

[33] Eisenhardt, K.M. and Graebner, M.E. (2007). Theory building from cases: Opportunities and challenges. Academy of Management Journal, 50(1), 25-32.

[34] Marshall, C. and Rossman, G.B. (2011). Designing Qualitative Research, 5th ed. Sage Publications, Thousand Oaks, CA.

[35] Patton, M.Q. (2014). Qualitative Research and Evaluation Methods: Integrating Theory and Practice. Sage Publications.

[36] Glaser, B.G. and Strauss, A.L. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine, Chicago.

[37] Guest, G., Bunce, A. and Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field Methods, 18(1), 59-82.

[38] Yin, R.K. (2018). Case Study Research and Applications: Design and Methods, 6th ed. SAGE Publications.

[39] Miles, M.B. and Huberman, A.M. (1994). Qualitative Data Analysis: An Expanded Sourcebook, 2nd ed. Sage Publications, Thousand Oaks, CA.

[40] Guba, E.G. and Lincoln, Y.S. (1994). Competing paradigms in qualitative research. In: Denzin, N.K. and Lincoln, Y.S. (Eds.), Handbook of Qualitative Research. Sage, Thousand Oaks, pp. 105-117.

[41] Strauss, A. and Corbin, J. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 2nd ed. Sage Publications.

[42] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017). Enterprise Risk Management: Integrating with Strategy and Performance. COSO, Washington, DC.

[43] Heroux, S. and Fortin, A. (2013). The internal audit function in information technology governance: A holistic perspective. Journal of Information Systems, 27(1), 189-217.

[44] Slapnicar, S., Vuko, T., Cular, M. and Drascek, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548.

[45] Vuko, T., Slapnicar, S., Cular, M. and Drascek, M. (2021). Key drivers of cybersecurity audit effectiveness: The neo-institutional perspective. SSRN Working Paper.

Appendix A. RESPONDENT DETAILS

Appendix A. Function, governance level, and background of respondents

Code	Function	Level	Background / Certifications
A1	Chief Operating Officer	Exec. management	Law; Management
A2	Chair, Audit and Risk Committee	Parent board	Commerce; GAICD
A3	Head of AI Risk and Compliance	2nd level	MSc IS; CISM; CRISC
A4	Chief Information Officer	2nd level	MEng Comp. Sci.; CISM
A5	AI/ML Engineer (Lead)	1st level	BSc Comp. Sci.; AWS ML
A6	IT Auditor	3rd level	BSc IT; CISA
A7	AI Product Manager	Exec. management	MBA; Data Science cert.
B1	Chief Technology Officer	2nd level	BEng Elec. Eng.; AI certs.

B2	Head of AI Governance	2nd level	MSc IS; CRISC
B3	Internal Audit Manager	3rd level	BCom; CISA; CISM
B4	Data Engineering Lead	1st level	BSc Comp. Sci.; MLOps
B5	Chief Risk Officer	Exec. management	BSc Mathematics; FRM
C1	Head of AI Development	1st level	MSc Comp. Sci.; CISSP
C2	Head of AI Risk	2nd level	BSc Chemistry; GRC cert.
C3	Chief Compliance Officer	Exec. management	LLB; data protection qual.
C4	IT Audit Lead	3rd level	BCom IS; CISA
C5	GCC Managing Director	Exec. management	MBA; experiential
C6	CISO	2nd level	MSc Info. Security; CISM
C7	Audit Committee Chair	Parent board	MCom Accounting; FCPA
C8	AI Platform Architect	1st level	BEng; cloud/AI arch. certs.
D1	AI/ML Operations Lead	1st and 2nd level	Vendor AI certifications
D2	IS Compliance	1st and 2nd level	BCom; CISA; CRISC
D3	CISO	Exec. management	Law enforcement; cybersecurity
E1	IT Auditor	3rd level	BSc Comp. Sci.; CISA; ISO 27001
E2	Group Risk Committee Chair	Parent board	MSc Physics; AI gov. training
E3	CISO / AI Risk Lead	2nd level	BSc Comp. Sci.; CISM; CISSA
E4	Chief Risk Officer	Exec. management	BBus Economics; FRM
E5	AI Systems Security Manager	1st level	BEng Elec. Eng.; ISO; ISACA

Appendix B. GIOIA DATA STRUCTURE

Appendix B. Gioia et al. [6] coding structure: first-order concepts, second-order concepts, and aggregate dimensions from 28 interviews

First-order concepts	Second-order concepts	Aggregate dimensions
AI asset dev. and training data management	1st level roles	Governance structure
Model deployment and MLOps operations	1st level roles	
Vendor API integration and tool onboarding	1st level roles	
Agentic AI prototype construction	1st level roles	
AI risk policy development and monitoring	2nd level roles	
Regulatory compliance mapping (DPDPA, CERT-In)	2nd level roles	
Approved AI tool registry management	2nd level roles	
AI incident detection and response	2nd level roles	
Shadow AI audit and detection	2nd and 3rd level	

AI governance maturity assessment	2nd and 3rd level	
Managing external AI assurance providers	3rd level roles	
Assurance of AI governance compliance	3rd level roles	
AI risk resource allocation	Exec. management	
AI risk appetite setting and endorsement	Exec. management	
Parent board oversight of AI risk	Parent board	
AI risk KRI feedback and challenge	Parent board	
Blended 1st/2nd AI governance tasks	1st and 2nd level	Relational mechanisms
Overdependence on CISO / AI Risk Lead	4th and 5th level	
Asymmetric AI literacy across levels	All levels	
External AI governance consultants	External providers	Mimetic forces
GCC industry benchmarking	External / industry	
Parent GRC tool and framework mandates	Parent organisation	
NIST AI RMF 1.0 [7]; ISO/IEC 42001 [13]	Professional frameworks	Normative forces
CISM, CRISC, CISA certifications	Professional certifications	
DPDPA 2023 enforcement [20]	Regulatory obligation	Coercive forces
CERT-In 6-hour reporting mandate [19]	Regulatory obligation	
SOC 2 Type II; ISO 27001 requirements	Standard compliance	
Parent AI governance mandates / directives	Parent organisation	
UEBA deployment mandated by parent HQ	Parent organisation	
AI portfolio size and complexity	Organisational factors	Efficiency/effectiveness motives
Multi-jurisdictional regulatory exposure	Environmental uncertainty	
AI delivery velocity pressure	Incentive structure	
Agentic AI governance policy absence	Governance gap	