

Emirati Journal of Business, Economics and Social Studies
Vol 5 Issue 2 (2026)
Pages 206 - 221
Available at
www.emiratesscholar.com

Governing the Capability-Accountability Gap through Global Capability Centres as Regulatory Nodes in the Gulf

Vipul V. Tamhane
Financial Regulatory Consultant, ExeSTAT Business Services Pvt Ltd, India

ARTICLE INFO

KEYWORDS
Global Capability Centres; regulatory accountability; legal pluralism; jurisdictional hybridity; AI governance; Gulf Cooperation Council

HOW TO CITE
Tamhane, V. V. (2026). Governing the Capability-Accountability Gap through Global Capability Centres as Regulatory Nodes in the Gulf. Emirati Journal of Business, Economics and Social Studies, 5(2), 206-221.
https://doi.org/10.54878/herfdx98

ABSTRACT

Global Capability Centres (GCCs), wholly-owned "captive" units through which multinational enterprises internalise offshore delivery, have migrated from cost-driven back offices toward research, engineering, artificial-intelligence (AI) development, cybersecurity and financial-control functions of global consequence. This article theorises the legal consequences of that migration in the Gulf, where the United Arab Emirates and Saudi Arabia have simultaneously constructed ambitious data- and AI-governance architectures. Its central and integrating claim is that when a GCC accumulates functional and technological capability faster than it acquires corresponding decision authority, legal responsibility and answerability, a Capability-Accountability Asymmetry emerges, producing a Regulatory Accountability Gap (RAG), a divergence between where consequential activity is performed and where legal answerability is located. The article makes four connected contributions. First, it develops the asymmetry into a Four-A model (capability, authority, responsibility, accountability) and operationalises the RAG through a diagnostic matrix and a set of threshold conditions, so that the gap becomes an analytical construct rather than a metaphor. Second, it offers a four-layer "Accountability Stack" (structural, operational, decision and behavioural) as a diagnostic instrument and applies it to a worked case. Third, it advances a four-stage "Regulatory Maturity Curve" on which RAG intensity rises during capability expansion and may fall as authority is re-allocated. Fourth, it reframes the "copy-paste" compliance error as Regulatory Translation Failure, grounded in legal-transplant theory, and reads the Saudi and Emirati regimes as two institutional solutions, centralised regulatory translation and polycentric regulatory reconciliation, to the same problem. Drawing on legal-pluralism, transplant, regulatory-intermediary and accountability scholarship and on doctrinal analysis of the relevant Gulf instruments, it conceptualises mature GCCs as sites of regulatory translation and co-production, and closes with boundary conditions, limitations and an agenda for empirical research.

Double-blind peer review by independent reviewers.
Received: 15 Jul 2026, Accepted: 21 Oct 2026, Published: 04 Nov 2026
*Corresponding author: vipul.tamhane@gmail.com
Copyright: © 2026 by the author. Licensee Emirates Scholar Center for Research & Studies, UAE.
Open access under the Creative Commons Attribution (CC BY) license
https://creativecommons.org/licenses/by/4.0

1. Introduction

The Global Capability Centre (GCC) has quietly become one of the most consequential organisational forms in the contemporary transnational economy, and one of the least theorised in law. Because the abbreviation "GCC" also denotes the Gulf Cooperation Council, this article reserves "GCC" for the Global Capability Centre and refers to the Gulf Cooperation Council and its member states as "the Gulf" or "the Gulf states." Conceived in the 1990s as the "captive" offshore centre - a wholly owned subsidiary through which a multinational enterprise (MNE) internalised routine processing rather than contracting it to a third-party vendor - the GCC was long understood as an instrument of labour arbitrage (Oshri et al., 2015). That understanding is now obsolete. Leading centres design products, own intellectual property, run cybersecurity operations, build and validate machine-learning models, and execute regulated financial functions such as transaction monitoring and sanctions screening (Gartner, 2024; Information Services Group [ISG], 2025; NASSCOM & KPMG, 2024).

This transformation has produced a governance paradox. The strategic significance of the GCC has grown faster than the legal and governance apparatus attached to it. The centre remains, in formal terms, a locally incorporated subsidiary - a distinct legal person subject to the company, data, labour and sectoral law of its host state - yet it is operationally and strategically fused with a parent that answers to an entirely different regulatory universe. The result is not merely "complex compliance." It is a structural divergence between where consequential activity now occurs and where legal answerability is located.

Nowhere is this divergence more analytically instructive than in the Gulf. The United Arab Emirates (UAE) and the Kingdom of Saudi Arabia have, within a compressed period, enacted comprehensive personal-data-protection statutes, established dedicated regulators, promulgated cross-border-transfer regimes and, in Saudi Arabia's case, issued a national AI risk-management framework and floated a first-of-its-kind draft law on sovereign "AI hubs." These are not developing jurisdictions passively importing Western templates; they are actively constructing their own digital-sovereignty architectures as instruments of national strategy (Kingdom of Saudi Arabia, 2016; Pohle & Thiel, 2020; Saudi Data and Artificial Intelligence Authority [SDAIA], 2020; United Arab Emirates Government, 2018). For an MNE that assumes its global compliance posture travels intact into Riyadh or Dubai, this is treacherous terrain.

The article's research question is: how does the emergence of the GCC as a strategically autonomous, technology-intensive organisational unit alter the allocation of regulatory accountability among the multinational parent, the host-state legal system and the local centre's own governance structures? Its central proposition is stated at the outset:

> *Global Capability Centres are evolving from geographically dispersed execution units into transnational decision-making and technology nodes. This transformation produces a Capability-Accountability Asymmetry: functional and technological capability increasingly resides within the GCC while decision authority, formal responsibility and answerability remain distributed among the host jurisdiction, the parent corporation and multiple regulatory regimes. This divergence creates a Regulatory Accountability Gap. Rather than treating that gap solely as a compliance deficiency, the article conceptualises mature GCCs as sites of regulatory translation and co-production, in which conflicting legal orders can generate new forms of adaptive governance.*

The novelty claim is precise. Existing scholarship addresses the constituent problems - legal pluralism, transnational corporate governance, regulatory intermediaries and the "governance gaps" of globalised business - largely in isolation, and has not trained those tools on the GCC as a distinct unit of analysis. This article integrates those strands through a GCC-specific Capability-Accountability Asymmetry framework and, crucially, operationalises the resulting Regulatory Accountability Gap through a diagnostic matrix, threshold conditions, a layered Accountability Stack and a maturity curve. It does not claim that GCCs are categorically unique legal entities; it claims that they are a particularly concentrated site at which the divergence between functional capability and formal accountability can be observed and theorised.

The article proceeds in five sections. Section 2 reviews the literature on capability centres, legal pluralism and legal transplants, sets out the theoretical framework and develops five propositions. Section 3 describes the research methodology. Section 4 presents the results: it situates the GCC doctrinally in the Gulf, develops the Capability-Accountability Asymmetry and the Four-A model, operationalises the Regulatory Accountability Gap, proposes the Accountability Stack and the Regulatory Maturity Curve, examines AI as an amplifier of accountability diffusion, compares the Saudi and Emirati governance models and discusses the findings.

Section 5 concludes with implications, limitations and an agenda for future research.

2. Literature Review

2.1 Global Capability Centres: From Cost Centres to Capability Hubs

The literature on global sourcing distinguishes the captive centre - a wholly owned offshore unit serving the group itself - from arm's-length outsourcing, in which an independent vendor performs the work under contract (Oshri et al., 2015). Early captive centres were justified by labour arbitrage and process standardisation. Recent industry evidence, however, records a sustained migration of function. The centre that a decade ago reconciled invoices now trains models, runs security-operations centres and owns parts of the group's product roadmap (Deloitte, 2025; EY, 2025; Gartner, 2024; ISG, 2025).

Four drivers push capability upward. Strategic function migration moves work from the back office to research and development, AI and cybersecurity. Technology ownership means that the centre increasingly builds proprietary systems and generates intellectual property that resides, at least nominally, in the local entity. Decision-making authority accrues as the centre performs model validation, risk analytics and compliance execution whose outputs bind the group. And regulatory exposure grows because the centre engages host-state regulators directly - registering as a controller, filing reports and answering supervisory queries. This literature documents the migration of capability well, but it treats the resulting governance questions as matters of operating model rather than of legal accountability, which is the gap this article addresses.

2.2 Legal Pluralism, Governance Gaps and Legal Transplants

Legal-pluralism scholarship establishes that a single actor may be subject simultaneously to multiple overlapping legal and quasi-legal orders, none simply supreme (Berman, 2012; Griffiths, 1986; Merry, 1988; Tamanaha, 2008). The GCC is an organisational manifestation of that condition. A related literature on the "governance gaps" of globalised business identifies the space that opens when economic activity outruns the reach of the legal orders that should govern it, typically across arm's-length supply chains (Levi-Faur, 2005; Ruggie, 2007; United Nations Human Rights Council, 2011).

Legal-transplant scholarship supplies the mechanism by which transferred rules fail or mutate in a new host. Watson's (1993) thesis that legal rules migrate readily between systems is met by Legrand's (1997) insistence that a rule, detached from the culture that gives it meaning, cannot truly be transplanted, and by Teubner's (1998) subtler account of transplanted rules as "legal irritants" that mutate in their new host and produce unintended divergence rather than convergence (see also Djelic & Sahlin-Andersson, 2006). Neither literature has yet been trained on the captive centre, in which the plural condition and the transplant problem arise inside a single owned entity.

2.3 Theoretical Framework: Regulatory Intermediation, Accountability and Co-production

Three further bodies of theory frame the analysis. First, regulatory-intermediary theory supplies the vocabulary for actors positioned between rule-makers and rule-takers, who interpret and transmit regulation rather than merely receive it (Abbott et al., 2017; Halliday & Shaffer, 2015). Second, accountability theory supplies the distinction, central to this article, between accountability as liability and accountability as answerability - the obligation to explain and justify conduct to a forum that can pass judgement on it (Bovens, 2007; Grant & Keohane, 2005; Scott, 2000). In polycentric regimes, in which regulatory authority is dispersed among several state and non-state actors, that answerability is itself fragmented (Black, 2008).

Third, the co-production idiom of science-and-technology studies holds that social-legal order and technical practice are produced together rather than sequentially (Jasanoff, 2004). Combined with the literature on responsive and staged regulation (Ayres & Braithwaite, 1992), it suggests that the governance of technology-intensive units should be understood as developmental rather than static. Together these literatures provide the building blocks for the framework developed in Section 4: pluralism explains why several orders meet in one centre, transplant theory explains how global rules fail there, intermediary and accountability theory explain where answerability should sit, and co-production explains how a mature centre can become a source of governance rather than only its object.

2.4 Propositions Development

Because the study is conceptual rather than statistical, it advances propositions rather than hypotheses for later empirical testing. The first follows from the accountability literature's separation of capability from answerability.

P1: Regulatory Accountability Gap (RAG) intensity increases where consequential capability is located

within the GCC but the corresponding decision rights, legal responsibility or answerability remain external to the centre or ambiguously allocated.

Because accountability operates in layers rather than at a single point of liability, the gap should concentrate where operational activity and decision authority come apart.

P2: The RAG is greatest where the centre's operational capability is high but its decision authority and its authority to resolve parent-host conflict remain external or ambiguous.

Responsive-regulation and co-production theory imply that the gap is developmental.

P3: RAG intensity is non-monotonic over a centre's life cycle: it rises during capability expansion and can decline as authority is reallocated to match capability.

Transplant theory implies that unadapted global rules generate mismatch, and automation lengthens the chain between action and answerability.

P4: Unadapted transfer of a parent's global compliance policy (Regulatory Translation Failure) widens the RAG, and AI-enabled decision-making amplifies it.

Finally, host-state institutional design should shape the form of the governance task but not the existence of the gap.

P5: Centralised host regimes frame GCC governance as regulatory translation into one dominant framework, whereas polycentric regimes frame it as reconciliation among overlapping orders; in both, a local regulatory overlay is required.

3. Research Methodology

3.1 Research Design

The article is a conceptual and comparative legal study. It combines four methods (Hutchinson & Duncan, 2012; Van Hoecke, 2015). It uses doctrinal analysis of the primary instruments governing capability centres in the Gulf - company, data-protection, anti-money-laundering and AI-governance law in the UAE and Saudi Arabia - to establish what the law actually does to the location of responsibility. It uses comparative legal method to set the Saudi and Emirati regimes against one another. It uses theoretical synthesis, drawing together the literatures reviewed in Section 2 - legal pluralism, legal transplants, regulatory intermediation and accountability theory - to build the framework. And it uses conceptual framework construction to convert the resulting insight into usable instruments: the Four-A model, the Regulatory Accountability Gap and its diagnostic matrix, the Accountability Stack and the Regulatory Maturity Curve.

3.2 Case Selection

The two-jurisdiction case selection is deliberate and limited. Saudi Arabia and the UAE are chosen not merely because they are the region's principal destinations for high-value capability-centre activity, but because they instantiate contrasting institutional models of data and AI governance - one centralised, one polycentric - and therefore offer the most analytically productive comparison for the argument. Other Gulf and global host jurisdictions are addressed briefly in Section 4.7 to test the framework's portability, not to provide exhaustive coverage.

3.3 Sources and Analytical Procedure

The primary materials are the Gulf statutes, regulations and official frameworks that govern personal data, companies, AML/CFT and AI, together with the draft Saudi Global AI Hub Law; each is cited to its official source in the reference list. Secondary materials comprise peer-reviewed scholarship and industry reports on capability centres. The analysis proceeds in three steps: each instrument is read for how it allocates duty, decision authority and answerability; the resulting allocations are compared across the two jurisdictions; and the comparison is used to construct and illustrate the diagnostic instruments, including a worked application. Because comprehensive decision-level enforcement reporting is not yet consistently published in Saudi Arabia, the analysis relies on the statutory enforcement architecture rather than on named decisions. The study draws only on publicly available documents and involves no human participants.

4. Results and Discussion

4.1 The GCC as a Legal Form and the Gulf Regulatory Environment

The Global Capability Centre as a legal form

A GCC is a captive, wholly owned offshore unit established by an MNE to perform functions for the group itself rather than for external clients. That single feature - ownership and control by the parent - is what distinguishes it, in law and in economics, from outsourcing. In an outsourcing relationship the MNE contracts with an independent vendor and allocates risk through a services agreement; the vendor bears primary regulatory responsibility for its own workforce, premises and processing. In the captive model the MNE internalises the activity: the people, systems and data sit inside a subsidiary the group owns, directs and

consolidates (Oshri et al., 2015). The consequence, frequently underappreciated at board level, is that offshoring the function does not offshore the regulatory obligation attached to it; this principle is treated here as the organising doctrinal premise of the captive model.

GCCs are typically constituted through one of a few legal vehicles: a wholly owned limited-liability subsidiary (the dominant form, offering separate legal personality and limited liability); a branch of the foreign parent (no separate personality, so the parent is directly exposed); or a Build-Operate-Transfer (BOT) arrangement in which a local provider establishes the centre and later transfers it to the MNE (Grand View Research, 2026; Oshri et al., 2015). Each vehicle distributes legal responsibility differently, yet all instantiate the same tension: a unit that is legally independent but operationally and strategically integrated. The subsidiary's separate personality is precisely what makes the accountability question hard: it is at once a shield the parent erects and an entity the parent controls in fact.

The United Arab Emirates

The UAE regulates personal data at two levels that counsel must hold in view simultaneously. Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the UAE PDPL) establishes the first comprehensive federal privacy regime, supervised by the UAE Data Office created under Federal Decree-Law No. 44 of 2021; it restricts cross-border transfers to jurisdictions offering an adequate level of protection or subject to prescribed safeguards, requires a data-protection officer for high-risk processing, and authorises administrative fines of up to AED 5 million (Federal Decree-Law No. 44, 2021; Federal Decree-Law No. 45, 2021). Gulf statutes and regulatory instruments are named in full at first mention and cited thereafter in short form (instrument number and year), with complete titles given in the reference list. Critically, the two principal financial free zones operate their own, separate data regimes: the Dubai International Financial Centre (DIFC) applies DIFC Data Protection Law No. 5 of 2020, and the Abu Dhabi Global Market (ADGM) applies its Data Protection Regulations 2021, each with its own commissioner and enforcement machinery; the federal PDPL does not apply within either zone (ADGM Data Protection Regulations, 2021; DIFC Data Protection Law, 2020). A centre's choice of domicile - mainland, a mainstream free zone, the DIFC or the ADGM - therefore selects not only a tax and licensing posture (Federal Decree-Law No. 47, 2022) but an entire data-governance order.

Corporate-governance obligations track a similar logic: directors of UAE companies owe statutory duties of care under Federal Decree-Law No. 32 of 2021 on Commercial Companies, and face joint civil liability for board decisions that cause loss unless their dissent is recorded in the minutes (Federal Decree-Law No. 32, 2021, arts. 22, 162). Sectoral regulation deepens rather than displaces this picture: a financial-services centre performing anti-money-laundering and counter-terrorist-financing (AML/CFT) monitoring is additionally subject to Federal Decree-Law No. 20 of 2018, under which the Central Bank of the UAE actively imposes personal and institutional penalties for control failures (Federal Decree-Law No. 20, 2018, art. 14).

The Kingdom of Saudi Arabia

Saudi Arabia's architecture is at once more centralised and more expansive. The Personal Data Protection Law (PDPL), issued by Royal Decree No. M/19 of 1443H (2021) and amended in 2023, entered into force on 14 September 2023 and became fully enforceable one year later. It is administered by the Saudi Data and Artificial Intelligence Authority (SDAIA), carries extraterritorial reach, and is elaborated by Implementing Regulations and a Regulation on Personal Data Transfer Outside the Kingdom, revised with standard contractual clauses and binding common rules and effective from September 2024 (Implementing Regulation of the Personal Data Protection Law, 2023; Personal Data Protection Law, 2021; Regulation on Personal Data Transfer Outside the Kingdom, 2024). Because SDAIA has not published an adequacy list, cross-border transfers presumptively require a prescribed safeguard rather than an adequacy shortcut (Regulation on Personal Data Transfer Outside the Kingdom, 2024). A Saudi centre performing AML/CFT functions answers to the Anti-Money Laundering Law issued by Royal Decree No. M/20 of 1439H (Anti-Money Laundering Law, 2017). Layered above this sits a fast-emerging AI-governance stack - SDAIA's AI Ethics Principles, its AI Adoption Framework, its National AI Risk Management Framework and the separately sponsored draft Global AI Hub Law - examined in Sections 4.6 and 4.7 (Communications, Space and Technology Commission [CST], 2025; SDAIA, 2023, 2025, 2026).

Two features matter for the argument. First, both jurisdictions have moved from regulatory readiness to active enforcement, so that the accountability question is no longer hypothetical (Federal Decree-Law No. 20, 2018; Personal Data Protection Law, 2021). Second, both frame data and AI governance not as technical housekeeping but as instruments of digital sovereignty and national competitiveness. Governance of a capability centre is, in this setting, adjacent to matters

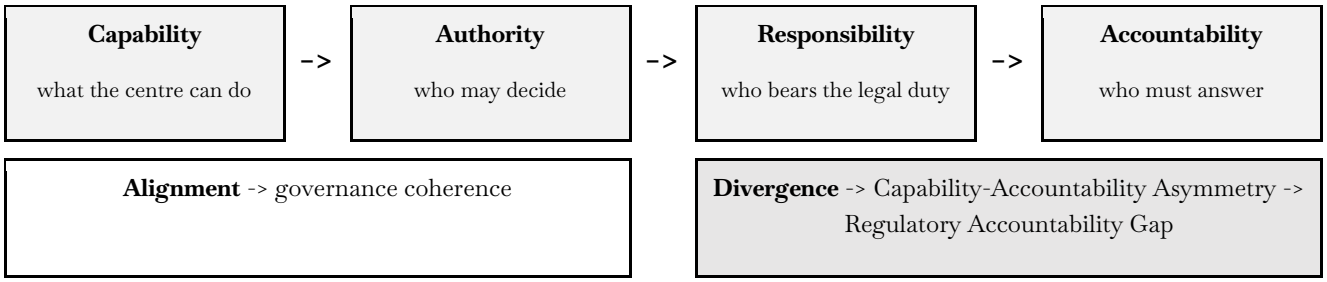
of state strategy. Where parent-company expectations (often calibrated to the EU General Data Protection Regulation [GDPR], US sectoral rules or UK governance codes), rapidly developing host-state requirements and the operational realities of continuous cross-border data flow overlap without coinciding, responsibility can fall between them. The remainder of this section names that space precisely and proposes instruments for governing it.

4.2 The Capability-Accountability Asymmetry and the Four-A Model

Legal accountability, unlike capability, is sticky. Corporate authority is allocated through instruments - articles of association, intra-group service agreements, delegation matrices and reserved-matter lists - that are revised infrequently and that tend to keep consequential authority formally at headquarters even as practical authority drifts to the centre. The centre may design and run an AI model end to end while the governing risk framework is "owned," on paper, by a committee abroad; it may hold the group's cyber-incident playbook while lacking authority to declare an incident. The divergence between de facto capability and de jure authority is the Capability-Accountability Asymmetry. Put formally: as capability (C) rises steeply while accountability (A) rises gently, the widening interval C – A is the Regulatory Accountability Gap (RAG).

The asymmetry is sharpened by disaggregating what "accountability" bundles together. Four distinct attributes, too often assumed to coincide, must be located separately: capability (who can perform the activity), authority (who is empowered to decide), responsibility (who is legally answerable in the sense of bearing the duty and its liability) and answerability, or accountability proper (who must explain and justify the outcome after the fact) (Bovens, 2007; Grant & Keohane, 2005; Scott, 2000). In a coherently governed unit these attributes align: the actor who can do the thing is authorised to decide it, bears the legal duty for it and must answer for it. The modern GCC governance problem is that they routinely do not. Capability migrates to the centre while authority, responsibility and answerability remain externally or ambiguously allocated. The RAG is best understood not as a single gap but as this misalignment among the four A's, and the misalignment explains why a fully compliant centre can still sit inside a wide gap: compliance speaks to whether controls exist, not to whether capability, authority, responsibility and answerability sit with the same actor. Figure 1 summarises the model.

Figure 1. The GCC accountability model



Note. Author's elaboration. Alignment of the four attributes produces governance coherence; divergence produces the Capability-Accountability Asymmetry and, in turn, the Regulatory Accountability Gap.

4.3 Operationalising the Regulatory Accountability Gap

If the RAG is to be more than an arresting phrase, it must be measurable in principle. The article therefore proposes a diagnostic matrix (Table 1) that pairs each consequential capability a centre may hold with the corresponding authority, responsibility and answerability that ought to accompany it. For each row, the analyst asks two questions: does the capability sit in the centre, and do the matching decision right and answerability sit there too? Divergence between the two columns is the observable signature of the gap.

Table 1. The Regulatory Accountability Gap diagnostic matrix

Capability located in the centre?	Corresponding authority/answerability located in the centre?
Strategic and product decision-making	Board-level or delegated decision rights; reserved-matter authority
AI development and model validation	Authority to approve model deployment and validate risk frameworks

Capability located in the centre?	Corresponding authority/answerability located in the centre?
Cybersecurity operations	Authority to declare and respond to a security incident
AML/CFT and sanctions analytics	Authority to file regulatory reports and make consequential compliance decisions
Intellectual-property creation	Authority to own, license, defend and retire the IP
Cross-border data processing	Authority to authorise transfers and select the lawful mechanism
Direct engagement with host regulators	Authority to answer, escalate and bind the entity in that engagement

Note. Author's elaboration. AML/CFT = anti-money laundering and counter-terrorist financing; IP = intellectual property.

The interpretive rule follows directly and restates Proposition P1: RAG intensity increases wherever consequential capability is located within the centre but the corresponding decision rights, legal responsibility or answerability remain external or ambiguously allocated. Stated this way, the gap is a testable construct. Its two variables, capability and accountability, can be scored against the rows of Table 1 for any given centre, and the divergence between them, rather than any single deficiency, is the quantity of interest.

The gap is not presumed to exist uniformly. A small captive centre doing payroll processing does not present the same problem as an AI, cybersecurity or AML centre. The RAG becomes analytically significant only when functional capability, technological autonomy or consequential decision-making exceeds the authority formally allocated to the local entity. Four threshold conditions can be distinguished (Table 2).

Table 2. Threshold conditions of the Regulatory Accountability Gap

RAG level	Capability and accountability profile	Illustrative centre
Low	Routine execution; authority clearly delegated and matched to activity	Payroll or back-office captive
Moderate	Specialised operational capability; local decision authority still limited	Analytics or shared-services centre
High	Strategic and technological capability; authority lags; decision rights external or ambiguous	AI, cyber or AML centre in capability expansion
Critical	Consequential automated decisions with cross-border exposure; legal answerability unclear or distributed	Autonomous AI-deploying centre

Note. Author's elaboration. RAG = Regulatory Accountability Gap. Thresholds are calibrated conceptually rather than empirically (see Section 5).

4.4 The Accountability Stack: A Layered Diagnostic

A flat compliance checklist cannot capture a gap that is fundamentally about the location of answerability, because accountability is a layered relationship of answerability rather than a single point of liability (Black, 2008; Bovens, 2007; Scott, 2000). The Accountability Stack comprises four analytically distinct layers. The layers are cumulative: a defect at a lower layer propagates upward, and most real-world failures arise not from the absence of any single layer but from a mismatch between them.

Layer 1 - Structural accountability: Who legally exists?

The foundational layer asks where legal responsibility formally resides: the entity's legal form; who owns it; who sits on its board; what authority has been delegated to, or reserved from, the parent; and where, in consequence, liability attaches. In the Gulf these questions have sharp doctrinal edges. Directors of a UAE company owe a statutory duty to act with the care of a "diligent person" and may incur personal, joint liability for damaging board decisions (Federal Decree-Law No. 32, 2021, art. 22). A centre constituted in the DIFC answers to different corporate and data authorities than one on the mainland. Structural accountability is necessary but never sufficient: a pristine capitalisation table and a well-composed board do not, by themselves, reveal who is answerable for what the centre actually does.

Layer 2 - Operational accountability: Who performs the regulated activity?

The second layer maps the centre's real operational footprint against the activities to which regulation attaches: personal-data processing, cybersecurity, AI deployment, employee management, financial controls, AML/CFT and sanctions screening, regulatory reporting, IP creation and third-party (vendor) management. This is where the captive model bites: because the activity is internalised, the regulatory obligation is internalised with it. A recurring failure is to treat vendor governance as procurement rather than as an operational-accountability discipline: a vendor being responsive is not the same as a vendor being compliant, and a sub-processor's lapsed licence becomes the centre's exposure.

Layer 3 - Decision accountability: Who makes the consequential decision?

The third layer is the one most often missing from both practice and scholarship, and it is the intellectual centre of the framework. It asks not who performs an activity but who owns the consequential decision within it: who approves the deployment of an AI model; who validates a risk framework; who authorises a cross-border data transfer; who decides how to answer a regulator. Decision accountability frequently fails to track either structural or operational accountability. The centre may perform the activity (Layer 2) and house the expertise while the decision right sits, formally, elsewhere - or, worse, is genuinely indeterminate. This is the layer at which the Four-A misalignment is most visible: capability present, authority absent.

Layer 4 - Behavioural accountability: Who resolves regulatory conflict?

The fourth layer is observable only under stress and cannot be fabricated in advance. It asks what leadership actually does when a parent instruction collides with host-state law - when group policy directs a data transfer that the host regime does not permit, or a global retention standard conflicts with a local erasure right. Does leadership escalate transparently, document the deliberation and resolve the conflict on the record, or does it attempt to satisfy both principals without acknowledging the tension, burying the conflict until enforcement surfaces it? Gulf company law supplies an unusually direct incentive for the disciplined version of this behaviour: because a UAE director escapes liability for a damaging majority decision only where the objection is recorded in the minutes, documented dissent is not merely good hygiene but a statutory shield, and documentation is the medium through which answerability is demonstrated (Bovens, 2007; Federal Decree-Law No. 32, 2021, art. 162). Behavioural accountability thus connects the softest governance question, institutional culture under pressure, to the hardest doctrinal consequence, personal liability. Table 3 summarises the four layers.

Table 3. The Accountability Stack as a diagnostic

Layer	Core question	Evidence	Characteristic failure
1. Structural	Who legally exists and bears liability?	Entity form, board, delegation matrix	Responsibility ambiguity
2. Operational	Who performs the regulated activity?	Processes, systems, vendor controls	Control mismatch
3. Decision	Who owns the consequential decision?	Approval matrices, reserved matters	Decision vacuum
4. Behavioural	Who resolves parent-host conflict?	Escalation records, minuted dissent	Accountability avoidance

Note. Author's elaboration.

The central diagnostic proposition (P_2) follows: the RAG is greatest where Layer 2 capability is high but Layer 3 decision authority and Layer 4 conflict-resolution authority remain external or ambiguous.

Worked application

Consider a Gulf-domiciled centre that develops and operates an AI model shaping credit or hiring decisions across several group markets. Applying the Stack makes the gap concrete. Layer 1: the centre is a locally incorporated subsidiary and the legal person of record. Layer 2: its engineers build, train and operate the model, so the regulated activity is internalised. Layer 3: deployment is "approved" by a parent committee abroad, so the consequential decision sits outside the centre. Layer 4: when the model produces an adverse, contestable outcome, it is local management that must answer the host regulator. Read through the Four-A lens, capability sits in the centre; the training data originate in Europe; the cloud substrate is controlled from the United States; approval authority sits with the parent; regulatory answerability lands locally; and legal

responsibility is distributed across all of them. No single legal order cleanly locates responsibility. The result is a High-to-Critical RAG on the threshold scale - not because any rule was broken, but because capability and answerability have come apart. The same analysis applies, with different rows engaged, to a centre performing AML transaction monitoring whose missed alerts carry consequences for regulated group entities in several states, and to a centre that holds valuable IP but lacks the decision rights to license, defend or retire it.

4.5 Regulatory Translation Failure and the Regulatory Maturity Curve

From "copy-paste" to Regulatory Translation Failure

Industry commentary routinely warns against the "copy-paste" of a parent's global compliance policy into a host jurisdiction. The metaphor is vivid but analytically thin. The precise defect is better named Regulatory Translation Failure: the transfer of a rule designed for one legal, institutional and enforcement environment into another without adaptation to local law, institutional structure, regulatory expectation and enforcement culture. The causal chain runs: global policy -> unmodified transplantation -> local legal mismatch -> control failure -> accountability ambiguity. A GDPR-shaped consent architecture, dropped unaltered into Saudi Arabia, may satisfy neither the PDPL's legal-basis requirements nor its transfer rules; and because SDAIA publishes no adequacy list, the parent's reflexive reliance on "adequacy" simply has no local analogue.

The GCC is thus a live site of the dynamic that Teubner (1998) describes: the parent's global control, transplanted, does not reproduce its home effect; it irritates the host system and is itself transformed (Levi-Faur, 2005). Regulatory Translation Failure is transplant theory operationalised for the compliance function, and it is the first limb of Proposition P4.

The Regulatory Maturity Curve

If the gap is developmental - capability outpacing accountability over time - the governance response must be developmental too. The article proposes a four-stage Regulatory Maturity Curve that replaces the static checklist with a lifecycle model, descriptive of how centres evolve and normative about what each stage demands. Consistent with Proposition P3, RAG intensity is not monotonic: it rises sharply during capability expansion and can decline once governance authority catches up, giving the model a dynamic rather than a merely cumulative shape (Ayres & Braithwaite, 1992; Black, 2008).

Stage I - Legal Establishment. "May we lawfully operate here?" The emphasis is on entity choice, ownership, licensing, board formation, employment, tax and initial data and IP arrangements. Accountability is overwhelmingly structural (Layer 1); the RAG is low.

Stage II - Operationalisation. "Can we operate compliantly?" Controls, internal audit, compliance, cybersecurity, data governance, third-party risk and reporting are embedded and exercised (Layer 2); the RAG is low to moderate.

Stage III - Capability Expansion. "What decisions can the centre now make?" As the centre develops AI, products, IP, financial models and strategic analytics, decision accountability (Layer 3) becomes the binding constraint, and the RAG typically opens widest here because capability sprints ahead of any reallocation of authority.

Stage IV - Regulatory Autonomy. "Is the centre a co-producer of governance?" A Stage IV centre possesses specialised compliance and legal capability, independent risk functions, its own AI-governance apparatus, direct regulatory relationships and genuine decision rights. Authority is reallocated to match capability, and the RAG can fall even as capability stays high.

Table 4 summarises the four stages and the RAG intensity expected at each.

Table 4. The Regulatory Maturity Curve and RAG intensity

Stage	Primary question	Governance emphasis	Expected RAG
I. Legal Establishment	May we lawfully operate here?	Entity, licensing, board, tax, initial data/IP (Layer 1)	Low
II. Operationalisation	Can we operate compliantly?	Controls, audit, cyber, data governance, reporting (Layer 2)	Low-Moderate
III. Capability Expansion	What decisions can the centre make?	AI, products, IP, financial models, risk systems (Layer 3)	High

Stage	Primary question	Governance emphasis	Expected RAG
IV. Regulatory Autonomy	Is the centre a co-producer of governance?	In-house legal/compliance, independent risk, AI governance, decision rights (Layers 3-4)	Potentially declining

Note. Author's elaboration. RAG = Regulatory Accountability Gap.

Stage IV is the article's most consequential claim and requires a qualification that the literature demands: to say that the centre "co-produces" governance is not to claim that GCCs are, in general, "regulatory innovators." That broad assertion is unsupportable. The defensible claim is narrower and, precisely because narrow, stronger: regulatory friction within a sufficiently mature GCC can become a site of institutional innovation. Faced with EU privacy requirements, the Saudi PDPL, UAE data rules, US group-security policy and parent AI governance that cannot be harmonised through any single global document, the centre is forced to develop jurisdiction-specific control overlays, data-localisation mechanisms, regulatory mapping and escalation protocols. Those local overlays can, in turn, be adopted at group level, so that host-state requirements indirectly reshape the multinational's global governance. The centre becomes, in that bounded sense, a laboratory for regulatory interoperability - an instance of the co-production of legal order and technical practice (Jasanoff, 2004; see also Kingsbury et al., 2005; Michaels, 2009).

4.6 AI and the Amplification of Accountability Diffusion

Three-directional exposure and diffusion

AI does not merely add another compliance domain; it changes the character of the accountability problem. The modern centre is exposed to AI in three directions at once: it builds AI internally for the parent; it consumes third-party AI to run its own operations; and it is increasingly asked to certify the lawfulness of both back to global leadership. Automated and semi-automated decision-making then distributes responsibility across a longer chain than human execution ever did. When an outcome is produced by a model, the candidates for accountability multiply - the parent that set the policy, the GCC board, local management, the data-protection officer, an AI-governance committee, the model owner, the vendor of a foundation model and the cloud provider - and each can point to another. AI is therefore properly described as an amplifier of the RAG rather than a new gap, as the second limb of Proposition P4 anticipates: it stretches the interval between capability and accountability by increasing the number of hands between an action and its author.

From human-in-the-loop to context-appropriate human control

It follows that the conventional demand for a "human in the loop" is too weak. Mere human presence does not close a Layer 3 decision gap; the relevant question is which human, possessing what authority and expertise, must intervene at which decision point, under what risk conditions and with what documented responsibility. The article therefore reframes the requirement as context-appropriate human control: human oversight matched to actual decision authority rather than to nominal presence, which operationalises the idea of accountability as answerability for automated decision-making (Bovens, 2007). On this view, AI governance is effective only when the human who can override the system also holds the authority to answer for the override - precisely the alignment the Four-A model demands.

The Gulf's emerging AI-governance overlay

The Gulf furnishes unusually concrete material against which to test this proposition. SDAIA's National AI Risk Management Framework, published in 2026, sets out a national methodology for identifying, assessing, treating and monitoring AI risk, organised around principles that expressly include transparency, privacy and accountability, and resting on the premise that AI risks differ from conventional software risks precisely because they may emerge unexpectedly, evolve over time and prove difficult to explain or reproduce (SDAIA, 2026). It is, by its own terms, advisory, layering on top of, rather than displacing, the binding PDPL, sectoral rules and SDAIA's AI Ethics Principles, whose accountability principle already fixes ethical responsibility on the designers, developers, owners, deployers and assessors of AI systems across the lifecycle (SDAIA, 2023). The UAE, by contrast, has pursued a more principles-based, innovation-forward posture, distributing AI-relevant obligations across the federal PDPL and free-zone regimes (Federal Decree-Law No. 45, 2021; United Arab Emirates Government, 2018). For a GCC, the practical upshot is that AI governance cannot live in a single global policy. It must be instantiated as a Layer 2 and Layer 3 discipline simultaneously: a written AI-use position that names the lawful basis under host law, fixes the IP and data-provenance stance, specifies context-appropriate human control and decision rights, and pre-commits an

escalation and breach pathway. AI governance, in short, is where the Accountability Stack and the Maturity Curve meet.

4.7 Two Models of Regulatory Governance: Saudi Centralised Translation and UAE Polycentric Reconciliation

The two leading Gulf destinations for capability investment have arrived at comparable ambitions by different regulatory routes. Read against the framework, they are not merely two privacy regimes but two institutional solutions to the same capability-accountability problem, as Proposition P5 anticipates.

Saudi Arabia represents a model of centralised regulatory translation. A single powerful authority, SDAIA, is at once the data regulator and the national reference point for AI, administering the PDPL and its Implementing and Transfer Regulations and issuing the AI Ethics Principles, the AI Adoption Framework and the National AI Risk Management Framework (Personal Data Protection Law, 2021; SDAIA, 2023, 2025, 2026). For a GCC, the governance task is accordingly framed as translating global corporate governance into a strong, concentrated host-state framework. The draft Global AI Hub Law extends this ambition into jurisdiction itself: opened for consultation by the Communications, Space and Technology Commission in April 2025, it proposes three categories of sovereign data centre - Private, Extended and Virtual "hubs" - and the novel device of the "data embassy," by which data hosted physically in the Kingdom may be governed by the law of a designated foreign state (CST, 2025). At the time of writing, the law remains a draft and should be described as a proposed, not an operative, framework. Its significance is conceptual: it is an explicit attempt to engineer jurisdictional hybridity by statute - capability in one territory, legal governance drawn from another - precisely the condition that this article theorises as arising informally within every GCC.

The UAE represents a model of polycentric regulatory reconciliation. Federal personal-data law coexists with the autonomous DIFC and ADGM regimes and with sectoral rules, and the AI posture emphasises enabling innovation while distributing responsibility across existing instruments rather than concentrating it in one authority (ADGM Data Protection Regulations, 2021; DIFC Data Protection Law, 2020; Federal Decree-Law No. 45, 2021). For a GCC, the governance task is not translation into a single dominant framework but reconciliation among multiple overlapping domestic orders - choosing the correct domicile and harmonising federal, free-zone and sectoral obligations while remaining integrated with global governance (Abbott et al., 2017; Black, 2008). Table 5 summarises the comparison.

Table 5. Two models of Gulf regulatory governance

Dimension	Saudi Arabia: Centralised translation	UAE: Polycentric reconciliation
Data governance	PDPL (Royal Decree No. M/19 of 1443H), SDAIA-administered; Implementing and Transfer Regulations	Federal PDPL (Federal Decree-Law No. 45 of 2021), UAE Data Office; separate DIFC and ADGM regimes
Cross-border transfer	SCCs and binding common rules; no published adequacy list	Adequacy determinations or prescribed safeguards
AI governance	SDAIA-centred: AI Ethics Principles, AI Adoption Framework, National AI Risk Management Framework	Principles-based national AI strategy; obligations distributed across instruments
Institutional design	Centralised (single dominant authority)	Polycentric (federal, free-zone and sectoral)
Sovereignty device	Draft Global AI Hub Law and "data embassies"	AI-hub ambition; domicile engineering across zones
GCC governance task	Translate global governance into one dominant framework	Reconcile multiple overlapping domestic orders

Note. Author's elaboration based on the instruments cited in Sections 4.1, 4.6 and 4.7. PDPL = Personal Data Protection Law; SCCs = standard contractual clauses.

In both jurisdictions a local regulatory overlay is unavoidable; only its shape differs. In neither is a transplanted global policy sufficient. And in both, the sovereignty framing draws the governance of capability centres into the domain of national strategic priority rather than private ordering. The framework is also portable beyond the Gulf. Comparable host-state regimes - the EU GDPR, India's Digital Personal

Data Protection Act 2023 and Qatar's Law No. 13 of 2016, the first comprehensive data-protection statute in the region - impose local requirements that no global policy can satisfy (Digital Personal Data Protection Act, 2023; General Data Protection Regulation, 2016; Law No. 13 on Protecting Personal Data Privacy, 2016). This is why the Capability-Accountability Asymmetry is a general feature of the GCC model, for which the Gulf is an especially instructive laboratory.

4.8 Discussion of Findings

The findings offer three principal insights. First, they give conceptual support to all five propositions. The doctrinal analysis shows that Gulf company, data and AML/CFT law attaches duties to the local entity and its directors (P_1); that the decisive divergence arises at the decision and behavioural layers rather than at the structural layer (P_2); that the gap is stage-dependent (P_3); that unadapted transfer and automation each widen it (P_4); and that Saudi centralisation and Emirati polycentricity change the governance task without removing the gap (P_5). This support is analytical rather than empirical, and the propositions remain to be tested.

Second, the findings clarify how four ideas that the analysis has kept in play relate to one another. Jurisdictional hybridity is a condition: multiple legal orders govern the same organisational activity. The Regulatory Accountability Gap is the problem that condition can produce: the location of capability does not correspond to the location of legal answerability. Regulatory Translation Failure is a mechanism by which the problem is realised: global rules are transferred into the host jurisdiction without adequate legal and institutional adaptation. Regulatory co-production is a potential governance response. Condition, problem, failure mechanism and response form a single architecture rather than four competing labels.

Third, the findings extend the three literatures reviewed in Section 2. The plural condition that pluralist scholarship locates in the external environment is here internalised within a single owned entity - a micro-pluralism in which host-state law, parent-state law, sectoral regulation, group policy and contractual governance meet inside one subsidiary (Berman, 2012; Griffiths, 1986). The "governance gap" arises within a single owned entity rather than across an arm's-length supply chain (Ruggie, 2007). And the GCC emerges not as a passive rule-taker but as an intra-organisational regulatory intermediary, positioned between the parent's governance architecture and the host legal order rather than between an external regulator and the firm (Abbott et al., 2017; Halliday & Shaffer, 2015).

Boundary conditions and counterarguments

Three objections merit a direct answer. First, it may be said that the Capability-Accountability Asymmetry is merely an ordinary corporate agency problem. It is not: agency theory addresses principal-agent incentives, whereas the RAG concerns the legal allocation of answerability, which is analytically distinct. A centre can have perfectly aligned incentives and still sit inside a wide gap because formal authority resides elsewhere (Bovens, 2007; Scott, 2000). Second, it may be said that the parent remains ultimately responsible, so that no gap exists. That objection confuses formal responsibility with operational decision accountability: ultimate parent responsibility does not tell the host regulator who was answerable for the consequential local decision. Third, it may be said that the phenomenon is not unique to GCCs. The article does not claim absolute uniqueness; it claims that captive ownership, functional integration, technological capability and cross-border regulatory exposure combine in the GCC to produce a particularly concentrated manifestation.

5. Conclusion

The Global Capability Centre has outgrown the vocabulary used to govern it. As a captive subsidiary it is legally local; as an operational unit it is transnational; as a technology owner it is increasingly global; and as a strategic asset it remains controlled from headquarters. That configuration makes it a jurisdictional hybrid in organisational form, and it produces a distinctive legal pathology: functional and technological capability accumulates faster than decision authority, legal responsibility and answerability are reallocated, so that answerability diverges from activity. This article has named that divergence the Capability-Accountability Asymmetry, sharpened as a misalignment among capability, authority, responsibility and accountability, and has named the gap it opens the Regulatory Accountability Gap, which it has operationalised through a diagnostic matrix and a set of threshold conditions rather than left as metaphor.

To govern this feature, the article has offered two instruments. The Accountability Stack disaggregates a flat compliance question into four layers - structural, operational, decision and behavioural - and locates most real failures in the mismatch between them, especially at the frequently missing decision layer; a worked case shows the diagnosis in operation. The Regulatory Maturity Curve replaces the checklist with a developmental model in which RAG intensity rises during capability expansion and can fall as authority is reallocated. Along the way, the article has reframed the "copy-paste" error as Regulatory Translation

ISSN: 2791-3171 - https://doi.org/10.54878/herfdx98

Failure; shown that AI amplifies accountability diffusion and that context-appropriate human control, not mere human presence, is what a Layer 3 gap requires; and read the Saudi and Emirati architectures as two models - centralised translation and polycentric reconciliation - of the same problem.

The study has practical implications. For regulators, calibrating governance expectations to a centre's maturity stage, rather than imposing a uniform checklist, better fits the phenomenon, provided that stage-sensitivity does not become a route to evasion; clear guidance on how host obligations interact with parent-state obligations would reduce the ambiguity the RAG describes, and regulators might recognise mature centres as sites of regulatory translation - a recognition that the draft Global AI Hub Law, whatever its fate, already gestures towards. For legal practitioners and corporate leaders, three disciplines follow: governance by design, because the captive model internalises regulated activity; localisation over replication, because a transplanted policy will not survive host scrutiny; and documentation as defence, because in an environment of active enforcement and personal director liability, minuted deliberations, recorded dissent, retained legal advice and evidenced risk assessments are the primary instruments by which decision and behavioural accountability are demonstrated. A compact diagnostic drawn from the Accountability Stack and the Maturity Curve appears in Appendix A.

The study has limitations. The framework is analytical, and its threshold scale is, as yet, calibrated conceptually rather than empirically; the comparison is confined to two jurisdictions; and Saudi enforcement practice is not yet documented at decision level. Future research could test the propositions through study of governance practice across Gulf jurisdictions and sectors; compare Gulf-based centres with centres in India, the Philippines and Eastern Europe to isolate what is distinctively "Gulf" about the accountability gap; trace longitudinally how AI deployment shifts the location of decision accountability; and analyse whether GCC governance standards might converge supranationally against the countervailing pull of digital sovereignty (Halliday & Shaffer, 2015; Kingsbury et al., 2005; Pohle & Thiel, 2020).

The final move is the one that makes the phenomenon worth studying rather than merely lamenting. At the mature end of the curve, the friction between irreconcilable legal orders does not only generate risk; it can generate capacity. A centre compelled to build overlays, mappings and escalation protocols that no single global policy could supply becomes a site of regulatory translation and co-production - an organisational venue in which host-state law is rendered into operational reality and, in turn, reshapes the group's global governance. As the Gulf continues to position data and AI governance at the centre of national strategy, the maturity of capability-centre governance ceases to be a back-office concern and becomes a strategic necessity, for the corporations that own these centres and for the states that host them alike.

Acknowledgements

The author has no acknowledgements to declare. This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors, and the author reports no competing interests. No new data were generated or analysed; the study draws entirely on publicly available primary documents and secondary literature, all of which are cited in the reference list. The research did not involve human participants, human data or animal subjects, and no ethical approval was required. The author is the sole and corresponding author and is responsible for the conception, research, analysis and writing of the article.

The manuscript was written entirely by the author. AI tools were used only for grammar and style checks, citation formatting and reference verification. All analysis, argumentation and framework development are original, and the author takes full responsibility for the content.

References

Abbott, K. W., Levi-Faur, D., & Snidal, D. (2017). Theorizing regulatory intermediaries: The RIT model. The ANNALS of the American Academy of Political and Social Science, 670(1), 14-35. https://doi.org/10.1177/0002716216688272

ADGM Data Protection Regulations 2021. (2021). Abu Dhabi Global Market. Retrieved from https://www.adgm.com/legal-framework

Anti-Money Laundering Law, Royal Decree No. M/20 of 1439H. (2017). Kingdom of Saudi Arabia. Retrieved from https://rulebook.sama.gov.sa/en/anti-money-laundering-law

Ayres, I., & Braithwaite, J. (1992). Responsive regulation: Transcending the deregulation debate. Oxford University Press. https://global.oup.com/academic/product/responsive-regulation-9780195070705

Berman, P. S. (2012). Global legal pluralism: A jurisprudence of law beyond borders. Cambridge University Press. https://doi.org/10.1017/CBO9781139028615

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & Governance, 2(2), 137-164. https://doi.org/10.1111/j.1748-5991.2008.00034.x

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447-468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Communications, Space and Technology Commission. (2025, April 14). Draft Global AI Hub Law [Public consultation draft]. Kingdom of Saudi Arabia. Retrieved from https://www.cst.gov.sa/en/media-center/news/N2025041401

Deloitte. (2025). 2025 Deloitte's Global Business Services (GBS) survey. Deloitte Insights. Retrieved from https://www.deloitte.com/ie/en/services/consulting/research/global-business-services-survey.html

DIFC Data Protection Law, DIFC Law No. 5 of 2020. (2020). Dubai International Financial Centre. Retrieved from https://www.difc.ae/business/laws-regulations/legal-database/data-protection-law-difc-law-no-5-2020/

Digital Personal Data Protection Act, No. 22 of 2023. (2023). Government of India. Retrieved from https://www.meity.gov.in/data-protection-framework

Djelic, M.-L., & Sahlin-Andersson, K. (Eds.). (2006). Transnational governance: Institutional dynamics of regulation. Cambridge University Press. https://doi.org/10.1017/CBO9780511488665

EY. (2025). Global Capability Center (GCC) pulse survey 2025. Ernst & Young LLP. Retrieved from https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/newsroom/2025/11/ey-global-capability-center-pulse-survey-november-2025.pdf

Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations. (2018). United Arab Emirates. Retrieved from https://uaelegislation.gov.ae/en/legislations/1016

Federal Decree-Law No. 32 of 2021 on Commercial Companies. (2021). United Arab Emirates. Retrieved from https://uaelegislation.gov.ae/en/legislations/1542

Federal Decree-Law No. 44 of 2021 on the Establishment of the UAE Data Office. (2021). United Arab Emirates. Retrieved from https://uaelegislation.gov.ae/en/legislations/2433

Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. (2021). United Arab Emirates. Retrieved from https://uaelegislation.gov.ae/en/legislations/1972

Federal Decree-Law No. 47 of 2022 on the Taxation of Corporations and Businesses. (2022). United Arab Emirates. Retrieved from https://mof.gov.ae/en/public-finance/tax/corporate-tax-in-the-uae/

Gartner. (2024, January 19). Consult the board: Strategy for global capability centers (GCCs). Gartner, Inc. Retrieved from https://www.gartner.com/en/documents/5129531

General Data Protection Regulation, Regulation (EU) 2016/679. (2016). Official Journal of the European Union, L 119, 1-88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Grand View Research. (2026). India GCC market size and share: Industry report, 2033 (Report No. GVR-4-68040-857-1). Retrieved from https://www.grandviewresearch.com/industry-analysis/india-gcc-market-report

Grant, R. W., & Keohane, R. O. (2005). Accountability and abuses of power in world politics. American Political Science Review, 99(1), 29-43. https://doi.org/10.1017/S0003055405051476

Griffiths, J. (1986). What is legal pluralism? The Journal of Legal Pluralism and Unofficial Law, 18(24), 1-55. https://doi.org/10.1080/07329113.1986.10756387

Halliday, T. C., & Shaffer, G. (Eds.). (2015). Transnational legal orders. Cambridge University Press. https://doi.org/10.1017/CBO9781107707092

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83-119. https://doi.org/10.21153/dlr2012vol17no1art70

Implementing Regulation of the Personal Data Protection Law. (2023). Saudi Data and Artificial

Intelligence Authority. Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx

Information Services Group. (2025). ISG Provider Lens: Global capability center (GCC) services - Global 2025 [Executive summary]. Retrieved from https://ei.isg-one.com/Research/_MarketingPage?dashboardID=201a11ca-c115-4a33-a9f7-941eceefbbd1&documentId=w4Lkto_EzX

Jasanoff, S. (Ed.). (2004). States of knowledge: The co-production of science and social order. Routledge. https://doi.org/10.4324/9780203413845

Kingdom of Saudi Arabia. (2016). Saudi Vision 2030. Retrieved from https://www.vision2030.gov.sa/en

Kingsbury, B., Krisch, N., & Stewart, R. B. (2005). The emergence of global administrative law. Law and Contemporary Problems, 68(3-4), 15-61. https://scholarship.law.duke.edu/lcp/vol68/iss3/2

Law No. 13 on Protecting Personal Data Privacy. (2016). State of Qatar. Retrieved from https://hukoomi.gov.qa/en/laws/law-no-13-of-2016-on-protecting-personal-data-privacy

Legrand, P. (1997). The impossibility of "legal transplants." Maastricht Journal of European and Comparative Law, 4(2), 111-124. https://doi.org/10.1177/1023263X9700400202

Levi-Faur, D. (2005). The global diffusion of regulatory capitalism. The ANNALS of the American Academy of Political and Social Science, 598(1), 12-32. https://doi.org/10.1177/0002716204272371

Merry, S. E. (1988). Legal pluralism. Law & Society Review, 22(5), 869-896. https://doi.org/10.2307/3053638

Michaels, R. (2009). Global legal pluralism. Annual Review of Law and Social Science, 5, 243-262. https://doi.org/10.1146/annurev.lawsocsci.4.110707.172311

NASSCOM & KPMG. (2024). GCCs in India: Building resilience for sustainable growth. NASSCOM. Retrieved from https://nasscom.in/knowledge-center/publications/gccs-india-building-resilience-sustainable-growth

Oshri, I., Kotlarsky, J., & Willcocks, L. P. (2015). The handbook of global outsourcing and offshoring (3rd ed.). Palgrave Macmillan. https://doi.org/10.1007/978-1-137-43744-0

Personal Data Protection Law, Royal Decree No. M/19 of 1443H. (2021, as amended 2023). Kingdom of Saudi Arabia. Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Documents/PersonalDataProtectionLaw.pdf

Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Regulation on Personal Data Transfer Outside the Kingdom. (2024). Saudi Data and Artificial Intelligence Authority. Retrieved from https://sdaia.gov.sa/en/SDAIA/about/ArchivesRegulationsAndPolicies/RegulationonPersonalDataTransferoutsideKingdomEN.pdf

Ruggie, J. G. (2007). Business and human rights: The evolving international agenda. American Journal of International Law, 101(4), 819-840. https://doi.org/10.1017/S0002930000037738

Saudi Data and Artificial Intelligence Authority. (2020). National strategy for data & AI. Retrieved from https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/NationalStrategyForDataAndAI.aspx

Saudi Data and Artificial Intelligence Authority. (2023). AI ethics principles. Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx

Saudi Data and Artificial Intelligence Authority. (2025). Artificial intelligence adoption framework. Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Files/AIAdoptionFramework.pdf

Saudi Data and Artificial Intelligence Authority. (2026). National AI risk management framework. Retrieved from https://www.spa.gov.sa/en/N2633781

Scott, C. (2000). Accountability in the regulatory state. Journal of Law and Society, 27(1), 38-60. https://doi.org/10.1111/1467-6478.00146

Tamanaha, B. Z. (2008). Understanding legal pluralism: Past to present, local to global. Sydney Law Review, 30(3), 375-411. https://classic.austlii.edu.au/au/journals/SydLawRw/2008/20.html

Teubner, G. (1998). Legal irritants: Good faith in British law or how unifying law ends up in new divergences. The Modern Law Review, 61(1), 11-32. https://doi.org/10.1111/1468-2230.00125

United Arab Emirates Government. (2018). UAE national strategy for artificial intelligence 2031. Retrieved from https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf

United Nations Human Rights Council. (2011). Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework (UN Doc. A/HRC/17/31). Retrieved from https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

Van Hoecke, M. (2015). Methodology of comparative legal research. Law and Method. https://doi.org/10.5553/REM/.000010

Watson, A. (1993). Legal transplants: An approach to comparative law (2nd ed.). University of Georgia Press. https://ugapress.org/book/9780820315324/legal-transplantspromulgated and it should be treated as a proposed rather than an operative framework.