WHITE PAPER

INDUS

Integrated National Digital Unified Standard

for Global Capability Centres

Why ISO Doesn't Fit GCCs, and Why India
Must Define Its Own Standard

One Certification. Eight Domains. Three Levels. One Badge.

Published by

Satyajit Dutta- CEO/Founder

Pithonix AI India Private Limited

Hyderabad, Telangana, India

For consideration by

NASSCOM | CII | MeitY | Bureau of Indian Standards (BIS)

April 2026 | Version 1.0

1. The Core Argument

India hosts 1,700 to 1,800+ Global Capability Centres employing approximately 1.9 to 2.0 million professionals, generating $64.6 billion in annual revenue (FY24). By 2030, these numbers are projected to reach 2,400 to 2,550 GCCs, 2.8 to 3.5 million professionals, and $105 billion in revenue. India accounts for over 53% of all GCCs globally.

Despite this scale, GCCs in India are currently evaluated and certified using ISO standards (ISO 9001, ISO 27001, ISO 22301, ISO 20000, and others) that were designed for fundamentally different types of organisations: independent companies with their own customers, their own governance, and their own P&L.

A GCC is none of those things. A GCC is a wholly owned captive entity of a parent corporation, operating as an extension of a global enterprise. Its governance is set abroad. Its customers are internal. Its financial model is based on transfer pricing, not market revenue. Its data flows across borders by design. Its talent operates under dual governance: Indian labour law and the parent company's global HR policies.

Applying ISO standards to this entity is like measuring a submarine with an aircraft's flight checklist. Both are engineering marvels. Both require rigorous standards. But the frameworks must match the operating reality.

This white paper proposes INDUS (Integrated National Digital Unified Standard), a purpose-built certification framework for Global Capability Centres. One certification that replaces the entire fragmented patchwork of ISO standards, SOC 2 reports, and regional/sector-specific certifications that GCCs are currently forced to maintain. INDUS covers the domains that existing standards miss entirely, and positions India as the global authority on GCC excellence.

2. Why Existing Certification Standards Do Not Fit GCCs

GCCs are currently evaluated using a patchwork of standards designed for fundamentally different types of organisations. ISO standards assume independent companies with external customers. SOC 2 assumes service organisations with vendor-client relationships. Sector-specific frameworks like HITRUST and PCI DSS assume standalone entities with defined compliance boundaries. A GCC is none of these things. This section examines each major standard and identifies the specific structural mismatches.

2.1 ISO 9001 (Quality Management) vs GCC Reality

ISO Assumption: The organisation has external customers and defines its own quality objectives.

GCC Reality: A GCC's "customer" is its parent company. Quality objectives are defined by the global headquarters, not by the India entity. ISO 9001 Clause 5.1.2 mandates "customer focus"

as a core requirement. When the customer is your own parent company and the relationship is governed by intercompany SLAs and transfer pricing agreements rather than market dynamics, the entire quality management framework is measuring the wrong relationship.

ISO Assumption: Top management commitment is demonstrated by the leadership of the certified entity.

GCC Reality: In a GCC, the strategic authority sits with global leadership in a different country and timezone. The India head executes a mandate. ISO audits the India entity in isolation, but the actual decision-making, risk appetite, and resource allocation happen 10,000 km away. The audit captures a fragment of the governance structure, not the whole picture.

2.2 ISO 27001 (Information Security) vs GCC Reality

ISO Assumption: The organisation defines its own Information Security Management System (ISMS) within a defined scope boundary.

GCC Reality: A GCC's data flows continuously between India and multiple global locations by design. The security perimeter is the parent's global infrastructure, not the India office. A Wells Fargo GCC in Hyderabad operates under US banking regulations (OCC, FDIC, SOX, GLBA), not just what ISO 27001 prescribes. An Eli Lilly GCC follows FDA 21 CFR Part 11 for data integrity. The GCC is already operating under sector-specific compliance regimes that are stricter and more specific than ISO 27001's generic controls.

The scope problem: ISO 27001 requires defining a "scope" for the ISMS. Auditing the India GCC in isolation creates an artificial boundary that doesn't reflect how data, access controls, and security incidents actually flow across the global enterprise. A breach at headquarters affects the GCC. A vulnerability in the GCC's network affects the parent. The scope boundary is a fiction.

2.3 ISO 22301 (Business Continuity) vs GCC Reality

ISO Assumption: The organisation plans for disruption to its own operations and its own customers.

GCC Reality: Business continuity for a GCC is bidirectional. If the parent company faces a disruption (a US banking crisis, a European regulatory action, a headquarters-level cyberattack), the GCC is directly impacted even if nothing happened in India. Conversely, a disruption at the GCC (natural disaster in Hyderabad, regulatory change in India, talent attrition spike) affects the parent's global operations. ISO 22301's framework is built for unidirectional BCM. GCCs need a framework that accounts for this mutual dependency and cross-border continuity planning.

2.4 What ISO Standards Miss Entirely

Beyond the mismatches in existing ISO standards, there are critical GCC-specific domains that no ISO standard covers at all:

- Cross-border data governance under multiple simultaneous jurisdictions (India's DPDP Act + EU GDPR + US state privacy laws + sector-specific regulations, all applying to the same data flowing through the same GCC).

- Talent ecosystem maturity in a dual-governed model (Indian labour law + parent company's global HR policies, compensation philosophy, diversity standards, and performance frameworks operating simultaneously).
- AI and digital readiness (over 70% of GCCs are implementing AI capabilities by 2026, with 58% investing in Agentic AI, but no certification standard evaluates AI governance, bias management, or autonomous decision-making in a GCC context).
- Innovation and value contribution measurement (how much is the GCC contributing to the parent's IP, product development, and strategic transformation vs simply executing back-office tasks).
- Transfer pricing compliance as a quality and governance indicator (the Union Budget 2026 standardised the safe harbour margin at 15.5% for IT/ITeS, directly affecting how GCC performance is measured and reported).

2.5 Beyond ISO: The SOC 2 and Regional Standards Problem

ISO certification is voluntary and not universally accepted as sufficient. In North America, which accounts for approximately 70% of GCC parent companies globally, SOC 2 Type II compliance has become the de facto standard for any entity handling sensitive data or operating within an enterprise supply chain. US enterprise clients and partners rarely accept ISO 27001 alone. They require SOC 2 reports.

SOC 2 (System and Organisation Controls) was developed by the American Institute of Certified Public Accountants (AICPA) and is built around five Trust Service Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. It is designed for service organisations, entities that provide services to other organisations.

A GCC, however, is not a service organisation in the SOC 2 sense. It is a wholly owned captive entity that serves its own parent company. It does not have the vendor-client relationship that SOC 2 was designed to govern. Yet because US-headquartered parent companies face SOC 2 requirements from their own customers and partners, these requirements cascade down to their GCCs regardless of fit.

The problem compounds further with regional and sector-specific standards:

- SOC 1 (SSAE 18): Required for GCCs handling financial reporting processes for US-listed parents. Overlaps with but does not replace SOC 2. Annual cost: Rs 8-15 Lakhs.
- HITRUST CSF: Required by many US healthcare organisations. Combines elements of ISO, NIST, HIPAA, and other frameworks into a healthcare-specific certification. Annual cost: Rs 15-30 Lakhs.
- PCI DSS: Required for any GCC processing, storing, or transmitting payment card data. Annual cost: Rs 5-15 Lakhs.
- CMMI (Capability Maturity Model Integration): Required for GCCs serving US defence or government contractors. Appraisal cost: Rs 10-20 Lakhs.

- Cyber Essentials / Cyber Essentials Plus: Expected by UK-headquartered parent companies for baseline cybersecurity assurance. Annual cost: Rs 2-5 Lakhs.
- C5 (Cloud Computing Compliance Criteria Catalogue): Required by German parent companies for cloud operations. Annual cost: Rs 8-15 Lakhs.
- ISO 27701: Privacy-specific extension of ISO 27001, increasingly demanded by EU parents for GDPR compliance attestation. Annual cost: Rs 4-8 Lakhs.
- CSA STAR (Cloud Security Alliance): Required by some parents for cloud-hosted GCC operations. Annual cost: Rs 3-8 Lakhs.

2.6 The True Cost: The Full Certification Stack

The table below shows what a mature GCC serving a US-headquartered parent company actually maintains. This is not a theoretical scenario. This is the daily reality for hundreds of GCCs in Hyderabad, Bengaluru, and Pune.

STANDARD	PURPOSE	ORIGIN	VOLUNTARY?	ANNUAL COST
ISO 9001:2015	Quality Management	Global	Yes	Rs 3-8 Lakhs
ISO 27001:2022	Information Security	Global	Yes	Rs 5-15 Lakhs
ISO 22301:2019	Business Continuity	Global	Yes	Rs 4-10 Lakhs
ISO 20000-1:2018	IT Service Mgmt	Global	Yes	Rs 4-10 Lakhs
ISO 31000:2018	Risk Management	Global	Yes	Rs 3-8 Lakhs
SOC 2 Type II	Security Trust Criteria	USA	De facto required	Rs 10-25 Lakhs
SOC 1 (SSAE 18)	Financial Controls	USA	Required for BFSI	Rs 8-15 Lakhs
HITRUST CSF	Healthcare Security	USA	Required for HC	Rs 15-30 Lakhs
PCI DSS	Payment Card Data	Global	Required if applicable	Rs 5-15 Lakhs
Cyber Essentials	Baseline Cybersecurity	UK	Expected by UK parents	Rs 2-5 Lakhs
FULL STACK TOTAL	7-10 separate audits	Mixed	Mixed	**Rs 50L - 1.2 Cr/yr**

Each certification requires its own audit cycle, its own documentation, its own internal team coordination, and its own management review process. For a 300-person GCC, this consumes hundreds of person-hours annually in preparation, evidence collection, audit facilitation, and remediation, all while measuring the organisation against frameworks that were designed for fundamentally different entities.

And here is the critical point: not a single one of these certifications evaluates AI governance in a GCC context, cross-border data compliance under multiple simultaneous jurisdictions, talent ecosystem maturity under dual HR governance, or innovation contribution from a captive centre to its parent organisation. The most important dimensions of GCC performance go entirely unaudited.

That is not a certification strategy. That is compliance theatre at scale.

INDUS replaces this entire fragmented stack with one unified certification that costs less, covers more, measures what actually matters, and is designed from the ground up for how GCCs actually operate.

3. Introducing INDUS: The Certification GCCs Actually Need

INDUS

Integrated National Digital Unified Standard
for Global Capability Centres

3.1 Why "INDUS"

The name INDUS carries deliberate significance. The Indus Valley Civilisation was one of the earliest examples of standardised urban planning, trade systems, and quality governance in human history. Weights, measures, and construction standards were unified across an entire civilisation, centuries before the concept of "standardisation" existed elsewhere.

India today finds itself in an analogous position with GCCs. It hosts over 53% of the world's Global Capability Centres. No other country comes close. If any nation has the authority, the data, and the operating experience to define a global standard for GCC excellence, it is India. INDUS is that standard.

3.2 Core Principles

- One certification replaces the entire patchwork: ISO standards, SOC 2, SOC 1, HITRUST, PCI DSS, Cyber Essentials, and other regional/sector-specific certifications. One audit cycle. One documentation framework. One badge.
- Built for captive entities, not independent companies. Every assessment criterion acknowledges that the GCC exists as an extension of a global enterprise, not as a standalone business.
- Cross-border by design. Data flows, governance chains, and compliance obligations across jurisdictions are assessed as they actually work, not within artificial scope boundaries.
- AI and digital maturity are first-class domains, not afterthoughts. In 2026, a GCC without AI governance is a liability. INDUS treats this as a core assessment area.
- Outcome-oriented, not documentation-oriented. INDUS evaluates what the GCC actually delivers (talent quality, innovation contribution, operational integration, security posture), not how many policy documents it has filed.

3.3 Three Certification Levels

LEVEL	CRITERIA	IDEAL FOR	VALIDITY
INDUS Ready	Meets baseline standards across all 8 domains. No critical gaps. Basic governance and security in place. Demonstrates intent and operational foundation.	New GCCs (0-2 years). Pilot-stage centres. GCCs in Tier 2/3 cities. Mid-market GCCs scaling up.	2 years

INDUS Certified	Full compliance across all 8 domains. Demonstrated maturity in governance, data integrity, talent management, and operational integration. Evidence-based assessment with measurable outcomes.	Established GCCs (2-5 years). Centres with 100+ employees. GCCs running multiple functions. Centres undergoing transformation.	3 years (with annual surveillance)
INDUS Prime	Highest tier. GCC operates as a true Centre of Excellence. Demonstrated innovation contribution, IP creation, global leadership roles, and measurable strategic impact on the parent organisation. Benchmark for the industry.	Mega GCCs (5,000+ employees). Centres operating at Portfolio/Transformation maturity. GCCs with global mandates. Innovation and R&D hubs.	3 years (with annual surveillance)

4. The Eight Assessment Domains of INDUS

Each domain below replaces or extends one or more ISO standards, while several domains cover areas that no ISO standard addresses at all. Together, the eight domains provide a complete, 360-degree assessment of GCC capability, maturity, and readiness.

Domain 1: Governance Alignment

Replaces elements of ISO 9001 (Quality Management)

This domain evaluates how well the GCC's governance structure aligns with the parent company's global framework while maintaining compliance with Indian regulatory requirements.

- Global-local governance mapping: clarity of decision rights between India leadership and global headquarters.
- Management mandate documentation: written mandates defining the GCC's scope, authority boundaries, and escalation protocols.
- Board and leadership structure: presence of India-based leadership with defined authority vs pure execution roles.
- Intercompany SLA framework: documented service level agreements between the GCC and the parent, with measurable KPIs.
- Transfer pricing compliance: alignment with India's safe harbour provisions (15.5% margin as per Union Budget 2026) and arm's length principles.
- Audit and reporting integration: how GCC reporting feeds into the parent's global audit, risk, and compliance framework.

Domain 2: Cross-Border Data Integrity

Replaces ISO 27001, SOC 2 Type II, and sector-specific security standards

This domain goes beyond ISO 27001's scope-limited ISMS to evaluate data governance across the full cross-border reality of a GCC.

- Multi-jurisdiction data classification: data categorised by which jurisdictions' laws apply (India DPDP Act, EU GDPR, US CCPA/state laws, sector-specific regulations).
- Cross-border data flow mapping: documented, auditable maps showing how data moves between the GCC and the parent, including third-party sub-processors.
- Global security posture integration: the GCC's security controls evaluated as part of the parent's global security architecture, not in isolation.
- Incident response across borders: documented protocols for security incidents that span jurisdictions, including notification obligations under different laws.
- Data localisation compliance: adherence to India's data localisation requirements where applicable.

- Sector-specific security controls: evaluation of banking (RBI guidelines), healthcare (HIPAA/NABH), or other sector-specific controls that the GCC must follow.

Domain 3: Talent Ecosystem Maturity

No ISO equivalent exists

This is a domain that ISO standards completely ignore, yet it is the single most critical factor for GCC success. Talent is what makes or breaks a GCC.

- Dual HR governance framework: documented structure showing how Indian labour law compliance and parent company global HR policies operate simultaneously.
- Employee Value Proposition (EVP) strength: measured attrition rates benchmarked against industry averages (GCCs pay 20-25% higher than non-GCC employers; the standard measures whether this premium translates to retention).
- Skilling and upskilling pipeline: investment in employee development, measured as percentage of payroll spent on learning, number of certifications achieved, and career progression rates.
- Diversity and inclusion metrics: workforce composition assessed against both Indian diversity benchmarks and the parent company's global D&I commitments.
- Leadership pipeline depth: percentage of leadership roles filled internally, number of India-based leaders holding global mandates.
- Employer brand positioning: measurable indicators of the GCC's attractiveness as an employer within its local talent market.

Domain 4: Operational Integration

Replaces elements of ISO 9001 + ISO 20000

This domain evaluates how deeply the GCC is integrated into the parent's global operations, going beyond traditional IT service management.

- Operational maturity stage assessment: classified as Cost Centre, Service Delivery Hub, Transformation Hub, or Portfolio/Innovation Hub (using established maturity models).
- Global process ownership: percentage of end-to-end global processes owned and run from the GCC (not just tasks, but full ownership).
- SLA adherence and service quality: measurable performance against intercompany SLAs with documented remediation for misses.
- Knowledge management and transfer: documented frameworks for knowledge continuity between GCC and parent, including succession planning for critical roles.
- Tool and platform standardisation: alignment of GCC's technology stack with the parent's global platforms (not shadow IT or local workarounds).

Domain 5: Regulatory Multi-Jurisdiction Compliance

Replaces SOC 1, PCI DSS, Cyber Essentials, C5, and other regional/sector standards

GCCs operate under multiple regulatory regimes simultaneously. No ISO standard evaluates this complexity.

- Regulatory mapping matrix: documented matrix showing all applicable regulations (Indian laws + parent country laws + sector-specific regulations) with assigned ownership for each.
- FEMA and RBI compliance: for GCCs receiving FDI, documented compliance with foreign exchange management and RBI reporting requirements.
- Indian labour code compliance: adherence to the four consolidated Labour Codes (implemented November 2025), including the new wage definition requiring basic pay to be at least 50% of total remuneration.
- Tax compliance architecture: transfer pricing documentation, safe harbour compliance, GST/TDS obligations, and alignment with India's evolving tax framework for GCCs.
- Industry-specific regulatory compliance: banking GCCs (RBI outsourcing guidelines), healthcare GCCs (CDSCO, NABH), pharma GCCs (FDA/EMA data integrity).

Domain 6: AI and Digital Readiness

No ISO equivalent exists

By 2026, over 70% of India's GCCs are implementing AI capabilities. 58% are investing in Agentic AI. Yet no certification standard evaluates AI governance, bias management, or autonomous decision-making in a GCC context. INDUS fills this gap.

- AI governance framework: documented policies for AI development, deployment, and monitoring within the GCC, aligned with both India's and the parent country's emerging AI regulations.
- AI use case inventory: catalogued list of all AI/ML deployments within the GCC with risk classification (low/medium/high) for each.
- Bias and fairness assessment: documented processes for evaluating and mitigating bias in AI models deployed or developed at the GCC.
- Human-in-the-loop protocols: for high-risk AI applications, documented requirements for human oversight, review, and override capability.
- Digital infrastructure maturity: cloud-native architecture adoption, API-first integration with parent systems, cybersecurity posture for AI/ML workloads.
- GenAI and Agentic AI governance: specific controls for large language model usage, autonomous agent deployment, and data privacy in generative AI contexts.

Domain 7: Business Continuity in Captive Model

Replaces ISO 22301 (Business Continuity Management)

Business continuity for a GCC is fundamentally different from an independent company because the dependency chain runs both ways.

- Bidirectional BCP: documented plans covering both "disruption at GCC affecting parent" and "disruption at parent affecting GCC" scenarios.
- Cross-border disaster recovery: DR infrastructure and failover plans that account for multi-location operations and jurisdictional constraints on data movement during emergencies.
- Geopolitical risk assessment: documented evaluation of geopolitical risks (trade restrictions, sanctions, visa/immigration policy changes, diplomatic tensions) that could affect GCC operations.
- Pandemic and hybrid work resilience: proven capability to maintain operations in distributed/hybrid work models, with documented lessons from past disruptions.
- Talent continuity planning: succession plans for critical roles, cross-training documentation, and knowledge retention strategies to mitigate attrition risk.

Domain 8: Innovation and Value Contribution

No ISO equivalent exists

This domain measures whether the GCC is actually contributing strategic value to the parent organisation, or simply executing tasks. It is the difference between a cost centre and a centre of excellence.

- IP contribution: patents filed, innovations documented, and proprietary methodologies developed at the GCC.
- Product and service innovation: GCC's contribution to the parent's product roadmap, measured by features/products conceived or built at the India centre.
- Revenue impact: quantifiable contribution to the parent's revenue growth, cost savings, or efficiency gains attributable to GCC-led initiatives.
- Strategic mandate expansion: evidence of the GCC taking on progressively higher-value mandates over time (from BPM to ER&D to global portfolio ownership).
- Ecosystem contribution: GCC's engagement with India's startup ecosystem (T-Hub, We-Hub, NASSCOM partnerships), academia (university collaborations, research partnerships), and government initiatives (skilling programs, CSR alignment).

5. INDUS vs the Current Certification Patchwork

PARAMETER	CURRENT PATCHWORK	INDUS (PROPOSED)
Certifications Required	7-10 (ISO + SOC 2 + SOC 1 + sector-specific)	1 unified certification
Annual Cost	Rs 50 Lakhs - Rs 1.2 Crore	Rs 25 - 55 Lakhs (one audit)
Audit Cycles	7-10 separate audit cycles/year	1 comprehensive audit/year
Designed For	Independent companies (ISO), service vendors (SOC 2), standalone entities (HITRUST/PCI)	Captive entities operating as extensions of global enterprises
Geographic Coverage	ISO (global but voluntary), SOC 2 (US), Cyber Essentials (UK), C5 (Germany)	One standard accepted across all parent-country contexts
Data Governance Scope	Single-entity ISMS with artificial scope boundary	Cross-border data flows across the full enterprise
Talent Assessment	Not covered by any standard	Full domain: dual HR governance, EVP, skilling, D&I, leadership pipeline
AI Readiness	Not covered by any standard	Full domain: AI governance, bias assessment, GenAI controls, Agentic AI
Multi-Jurisdiction Compliance	Not covered by any standard	Full domain: DPDP + GDPR + sector-specific + tax + labour codes
Innovation Measurement	Not covered by any standard	Full domain: IP, product contribution, revenue impact, mandate expansion
Business Continuity Model	Unidirectional (own disruption)	Bidirectional (mutual dependency with parent)
Transfer Pricing Relevance	Not addressed	Integrated as governance and compliance indicator
Geopolitical Risk	Not addressed	Assessed as business continuity factor
Certification Levels	Pass/Fail per standard	Three tiers: Ready, Certified, Prime
Assessment Approach	Documentation-heavy, process-oriented	Outcome-oriented, evidence-based
Captive Entity Fit	Designed for vendors and independent orgs	Designed specifically for wholly owned captive centres

6. Governance Structure: Who Should Own INDUS

INDUS must be governed by a body that carries institutional weight, industry credibility, and government backing. The following governance structure is proposed:

6.1 The INDUS Council

A multi-stakeholder body comprising:

- NASSCOM: As the apex body for India's IT and BPM industry, NASSCOM is the natural anchor. NASSCOM already publishes GCC landscape reports, runs the GCC Summit, and works closely with state governments on GCC policy. NASSCOM's involvement lends immediate industry credibility.
- Bureau of Indian Standards (BIS): As India's national standards body and ISO member, BIS provides the formal standardisation infrastructure. BIS involvement ensures INDUS can be structured as a formal Indian Standard (IS) with potential for submission to ISO as a new work item proposal.
- CII (Confederation of Indian Industry): CII has already proposed a National GCC Policy Framework. Their involvement ensures alignment with broader industrial policy advocacy.
- MeitY (Ministry of Electronics and IT): Government backing ensures policy alignment and potential integration with national digital infrastructure initiatives.
- GCC Industry Representatives: A rotating panel of GCC heads from across verticals (BFSI, Healthcare, Technology, Manufacturing) providing practitioner input.

6.2 Certification Body Structure

- Accredited auditor network: third-party auditors trained and accredited specifically for INDUS assessments (similar to how ISO 27001 auditors require IRCA or equivalent certification).
- Annual auditor calibration: standardised assessment criteria updated annually to reflect evolving regulations, technology shifts, and industry benchmarks.
- Digital audit infrastructure: assessments conducted through a digital platform (not paper-based), enabling real-time evidence collection, automated scoring, and benchmarking against anonymised peer data.

7. Path to Adoption

PHASE	TIMELINE	ACTIONS	OUTCOME
Phase 1	Month 1-4	White paper socialisation with NASSCOM, CII, BIS, and MeitY. Roundtable with 20-30 GCC heads across verticals. Formation of INDUS Working Group.	**Working Group Formed**
Phase 2	Month 5-10	Detailed standard development. Domain-by-domain assessment criteria with scoring methodology, evidence requirements, and maturity level definitions. Industry review and feedback.	**Draft Standard Published**
Phase 3	Month 11-14	Pilot certifications with 10-15 volunteer GCCs across BFSI, Healthcare, Technology, and Manufacturing verticals. Pilot across Hyderabad, Bengaluru, Pune. Auditor training programme.	**Pilot Complete**

Phase 4	Month 15-18	Standard refinement based on pilot feedback. Formal publication through BIS or NASSCOM. Auditor accreditation programme launched. First official INDUS certifications issued.	**INDUS Live**
Phase 5	Month 19-24	National rollout. Integration with state GCC policies (Karnataka, Telangana, Maharashtra, UP). Engagement with ISO/TC for potential new work item proposal to develop a global GCC standard based on INDUS.	**National Standard**

8. Pithonix AI's Role in INDUS

Pithonix AI proposes to serve as the technical architect and digital infrastructure provider for INDUS, not as the governing body (which rightly belongs to NASSCOM/BIS/CII), but as the technology engine that powers the standard's implementation.

- Digital Assessment Platform: Pithonix builds the digital infrastructure for INDUS assessments, leveraging its existing GOT (Graph of Thought) engine which already reasons across 8 domains for GCC decision-making. The same 8-domain architecture maps directly to the INDUS assessment framework.
- JEET Framework Integration: Pithonix's JEET (Just-in-time, Emotionally Empowered Technology) ERP can serve as the continuous compliance monitoring layer for INDUS-certified GCCs, providing real-time dashboards showing domain-by-domain compliance status rather than point-in-time annual audits.
- INDUS Readiness Simulator: built into the existing GCC Playbook at gcc-playbook.pithonix.ai, allowing GCCs to self-assess their readiness against INDUS criteria before engaging with a formal auditor.
- Auditor Training and Calibration Platform: a digital platform for training and certifying INDUS auditors, ensuring consistency across the auditor network.

Pithonix does not seek to own the standard. Standards must be industry-governed and publicly accessible to gain trust and adoption. Pithonix's role is to provide the technology that makes INDUS practical, scalable, and digitally native from day one, rather than paper-based like legacy certification frameworks.

9. The Bigger Picture: India's Moment to Lead

India accounts for over 53% of the world's Global Capability Centres. No other country comes close. The Philippines, Poland, and other GCC destinations combined don't match India's scale, maturity, or ecosystem depth.

Yet when it comes to standards and certifications, India's GCCs follow frameworks designed in Geneva by organisations that have never audited a captive centre in Hyderabad or evaluated cross-border data flows between Mumbai and Manhattan.

This is not about rejecting ISO. ISO standards have served global industry well for decades, and they continue to be valuable for independent companies operating in traditional structures. But GCCs are not traditional structures. They are a new organisational form that emerged at scale over the past decade, and India is where that scale lives.

INDUS is India's opportunity to do what it did with UPI for payments, what it did with Aadhaar for identity, and what it did with CoWIN for vaccination: build a digital-first standard that the rest of the world eventually adopts because it simply works better for the problem it was designed to solve.

The question is not whether a GCC-specific certification standard will emerge. It will, because the mismatches documented in this white paper are too significant to ignore as the sector grows towards $105 billion. The question is whether India will lead its creation, or wait for someone else to define it.

INDUS: One Certification. Eight Domains. Three Levels. One Badge.

Designed for GCCs. Defined by India. Ready for the World.

10. Contact

Satyajit Dutta

Founder & CEO, Pithonix AI India Private Limited

Email: Satyajit.d@pithonix.ai, info@pithonix.ai

Platform: pithonix.ai

GCC Playbook: gcc-playbook.pithonix.ai

Location: Hyderabad, Telangana, India