

Overcoming Regulatory Fragmentation in Cross-Border Data Flows: An Inclusive Framework for the Belt and Road Initiative

Tao Wu¹

¹ Al-Farabi Kazakh National University, Almaty 050040, Republic of Kazakhstan

Correspondence: Tao Wu, Al-Farabi Kazakh National University, Almaty 050040, Republic of Kazakhstan.

doi:10.63593/SLJ.2026.06.07

Abstract

The Belt and Road Initiative (BRI) faces a critical bottleneck in realizing seamless cross-border data flows: deep regulatory fragmentation across participating jurisdictions. Divergent legal traditions, data governance philosophies, and institutional capacities impede interoperability, erode trust, and constrain digital cooperation. This paper proposes an Inclusive Framework—a tiered, modular rule architecture designed to reconcile developmental asymmetry with systemic coherence. Drawing conceptual and structural insights from the Digital Economy Partnership Agreement (DEPA) and the Regional Comprehensive Economic Partnership (RCEP), the framework operationalizes three foundational principles—inclusiveness, security, and gradualism—through layered commitments, opt-in modules, and phased implementation pathways. It enables countries at varying stages of digital maturity to participate meaningfully without compromising core sovereignty or essential safeguards. The design prioritizes legal interoperability over harmonization, allowing domestic regulatory autonomy while establishing shared baseline standards for data transfer integrity, accountability, and redress. By decoupling ambition from uniformity, the framework offers a pragmatic, politically viable pathway toward resilient, equitable, and scalable digital connectivity across the BRI space.

Keywords: Belt and Road Initiative, data governance, regulatory fragmentation

1. Introduction: The Regulatory Chasm in BRI Digital Integration

1.1 *The Data Flow Imperative and Its Institutional Obstacle*

Cross-border data flows constitute a foundational enabler of the Belt and Road Initiative's economic integration, digital infrastructure interoperability, and innovation diffusion objectives (F. Hussain, A. Imran, Z.

Hussain, & M. I. Khan., 2023; X. Sun, L. Li, L. Yuan, Y. Song, & D. Zhang, 2026). Yet their realization is systematically impeded by regulatory fragmentation across BRI jurisdictions—arising from divergent legal traditions, data governance philosophies, institutional capacities, and developmental priorities. This chasm manifests in incompatible data localization mandates, asymmetrical consent frameworks, heterogeneous

cybersecurity standards, and inconsistent enforcement mechanisms (M. S. Erie & T. Streinz, 2022). Such heterogeneity not only increases transaction costs for multinational enterprises but also undermines trust among participating states, constrains public-sector digital cooperation, and inhibits scalable platform-based service delivery. Conventional harmonization approaches prove inadequate given the vast disparities in legal maturity, technological readiness, and policy autonomy among BRI members. Consequently, the imperative shifts toward institutional architecture that embraces pluralism without sacrificing coherence—where rule design acknowledges developmental gradients while preserving functional interoperability (X. Changdeng & Y. Shumei., 2025; C. Nalbantoğlu., 2022). The central challenge lies in constructing governance scaffolds capable of accommodating normative diversity without enabling regulatory arbitrage or systemic disintegration. A viable pathway must therefore reconcile inclusiveness with enforceability, security with openness, and ambition with feasibility—grounding regional digital integration in principles of gradualism, mutual recognition, and modular scalability (F. Hussain, A. Imran, Z. Hussain, & M. I. Khan., 2023; O. Borgogno & M. S. Zangrandi, 2025).

1.2 Beyond Harmonization: Why Uniform Rules Fail in Heterogeneous Jurisdictions

Top-down harmonization models presuppose a convergence of legal epistemologies, institutional capacities, and developmental timelines—conditions demonstrably absent across Belt and Road jurisdictions. Uniform rule imposition disregards the ontological divergence between civil law traditions emphasizing codified certainty, common law systems privileging precedent-based adaptability, and hybrid regimes shaped by postcolonial institutional legacies (F. Hussain, A. Imran, Z. Hussain, & M. I. Khan, 2023). Such models also ignore asymmetries in regulatory enforcement infrastructure: where some states possess robust data protection authorities with investigative powers and judicial review mechanisms, others operate under fragmented oversight with limited technical capacity for compliance monitoring. Moreover, developmental priorities vary significantly—some nations prioritize digital sovereignty and local content mandates, while others emphasize market access and interoperability (X. Changdeng & Y. Shumei,

2025; Y. Zhao. (Ed.), 2018). These disparities render rigid harmonization politically unfeasible and technically unsustainable. Instead, effective regional integration requires normative architectures that acknowledge heterogeneity as constitutive rather than incidental. A viable framework must therefore embed flexibility into its foundational design—not as an afterthought, but as a structural principle—enabling differentiated implementation pathways without compromising core functional objectives such as cross-border data integrity, accountability, and mutual recognition.

1.3 Core Proposition: An Inclusive Framework as a Structural Alternative

This paper advances an Inclusive Framework for the Belt and Road Initiative that directly confronts regulatory fragmentation in cross-border data governance. Rather than pursuing harmonization—a normatively and practically unattainable objective across jurisdictions with divergent legal traditions, institutional capacities, and developmental priorities—the framework proposes a tiered, modular architecture (M. S. Erie & T. Streinz, 2022). Inspired by the adaptive rule design of the Digital Economy Partnership Agreement and the RCEP's differentiated implementation pathways, it embeds three foundational principles: inclusiveness through opt-in modules calibrated to national readiness levels; security via interoperable baseline standards for data integrity, accountability, and redress; and gradualism through phased compliance timelines and mutual recognition mechanisms that evolve with domestic regulatory maturation (F. Hussain, Z. Hussain, M. I. Khan, & A. Imran, 2024). Crucially, the architecture avoids mandating legal convergence, instead enabling functional equivalence across heterogeneous systems. Each module—covering data localization, cross-border transfer conditions, algorithmic transparency, and dispute resolution—is designed as a self-contained unit, permitting countries to adopt, adapt, or defer based on sovereign capacity and policy preference (A. He., 2023; H. Guo, J. Liu, Y. Qiu, M. Menenti, F. Chen, P. F. Uhler, et al., 2018). This structural flexibility ensures scalability without diluting core safeguards, thereby transforming regulatory diversity from a barrier into a design parameter for sustainable digital integration (X. Changdeng & Y. Shumei., 2025).

2. Literature Review: Gaps in Global Digital

Governance and Regional Experimentation

2.1 Fragmentation Studies: From Legal Pluralism to Operational Disruption

Regulatory fragmentation in cross-border data governance manifests not merely as doctrinal divergence but as operational friction that escalates compliance costs, distorts investment horizons, and erodes cooperative trust across jurisdictions (X. Changdeng & Y. Shumei., 2025). Scholarship increasingly frames this fragmentation as a structural impediment rather than a transient coordination challenge—highlighting how heterogeneity in data localization mandates, consent architectures, and enforcement mechanisms generates cumulative uncertainty for multistakeholder actors (Y. Zhao. (Ed.), 2018). Legal pluralism, while theoretically enriching, translates empirically into jurisdictional arbitrage, regulatory duplication, and asymmetric implementation burdens, particularly for small-and medium-sized enterprises operating across BRI corridors. Existing global instruments lack adaptive granularity to accommodate differential institutional capacities, developmental priorities, and digital infrastructure maturity. Consequently, rule-making processes often default to lowest-common-denominator standards or exclusionary harmonization, neither of which sustains long-term participation or interoperability. This literature underscores a critical gap: the absence of scalable, modular frameworks that embed inclusiveness, security, and gradualism as foundational design principles—not ancillary considerations (F. Hussain, Z. Hussain, M. I. Khan, & A. Imran, 2024). Without such architecture, regulatory divergence risks calcifying into systemic barriers that impede data-enabled trade, innovation diffusion, and public service integration across the BRI ecosystem. Furthermore, this regulatory fragmentation extends profoundly into the realm of intellectual property (IP) law. Divergent national IP regimes create fundamental legal frictions between mandates for open data sharing and the robust protection of algorithmic trade secrets. When multinational enterprises transfer data across BRI corridors, the lack of a harmonized mechanism to allocate derivative IP rights—specifically regarding AI models trained on transnational datasets—exacerbates operational reluctance. Without modular IP guidelines that reconcile proprietary technical protections with cooperative data governance,

regulatory divergence will continue to constrain high-value digital integration.

2.2 Lessons from RCEP and DEPA: Modularity, Asymmetry, and Opt-In Logic

Recent plurilateral agreements demonstrate how modular architecture can reconcile regulatory heterogeneity without compromising systemic coherence (O. Borgogno & M. S. Zangrandi, 2025). The Regional Comprehensive Economic Partnership embeds core digital trade disciplines within its main text while delegating technical implementation to annexes and side letters, enabling differentiated compliance timelines and capacity-building pathways. Similarly, the Digital Economy Partnership Agreement adopts an opt-in framework where parties selectively accede to modules on artificial intelligence governance, data trust frameworks, or cross-border data certification—each with self-contained definitions, obligations, and review mechanisms (F. Hussain, Z. Hussain, M. I. Khan, & A. Imran, 2024; A. He., 2023). Both instruments institutionalize asymmetry not as exception but as design principle: obligations scale with national readiness, enforcement mechanisms adapt to domestic administrative capacity, and dispute resolution pathways reflect jurisdictional maturity. Crucially, neither prescribes uniform legal transposition; instead, they permit functional equivalence assessments, allowing diverse statutory forms to satisfy shared policy outcomes (F. Hussain, A. Imran, Z. Hussain, & M. I. Khan., 2023; A. He., 2023). This tiered logic—where foundational principles anchor flexible implementation layers—offers a replicable template for BRI governance. It supports gradualist integration by decoupling normative consensus from immediate legislative harmonization, thereby reducing entry barriers for developing economies while preserving interoperability across jurisdictions with divergent legal traditions and digital infrastructure endowments (A. He, 2023).

2.3 The Missing Link: Bridging Developmental Justice and Technical Interoperability

Scholarship on digital governance consistently identifies regulatory fragmentation as a structural impediment to cross-border data flows, yet remains largely silent on institutional pathways that reconcile developmental heterogeneity with technical interoperability (C. Nalbantoğlu, 2022; F. Hussain, Z. Hussain, M. I. Khan, & A. Imran, 2024). Normative appeals for

inclusivity frequently lack operational specificity, failing to articulate how differential capacity—legal, infrastructural, or administrative—can be systematically accommodated within binding rule frameworks. Existing regional agreements demonstrate divergent approaches: some prioritize harmonization through top-down standardization, while others rely on opt-in flexibility without enforceable scaffolding for convergence. This leaves a critical void between abstract equity commitments and implementable modular architecture. The missing link lies in designing tiered rule layers—core principles, adaptive modules, and staged implementation protocols—that permit differentiated compliance timelines, capacity-building triggers, and jurisdictional carve-outs without undermining systemic coherence. Such architecture must embed gradualism not as concession but as design logic: rules evolve in tandem with domestic institutional maturation, ensuring security thresholds remain non-negotiable while procedural pathways remain scalable (X. Sun, L. Li, L. Yuan, Y. Song, & D. Zhang, 2026). Without this linkage, inclusivity risks devolving into rhetorical abstraction rather than functional interoperability (H. Guo, J. Liu, Y. Qiu, M. Menenti, F. Chen, P. F. Uhlir, et al., 2018).

3. Methodology: Designing for Inclusiveness—A Structured Architectural Approach

3.1 Principle-Driven Architecture: Defining Inclusiveness, Security, and Gradualism

As illustrated in Figure 1, the Triadic Principle Architecture establishes a logically interdependent framework wherein Inclusiveness, Security, and Gradualism operate not as discrete ideals but as mutually reinforcing design axioms. Inclusiveness functions as the foundational enabler of opt-in modularity and sovereign choice, permitting states to select only those regulatory modules aligned with domestic legal capacity and policy priorities. Security constitutes the non-derogable baseline—defining minimum interoperability thresholds for data localization, cross-border transfer mechanisms, and redress procedures that all participating jurisdictions must satisfy prior to accession. Gradualism operationalizes time-bound, capacity-triggered phasing: progression to higher-tier modules is contingent upon verifiable institutional upgrades, such as judicial training benchmarks or digital infrastructure indices. Crucially, bidirectional reinforcement arrows indicate that sovereign choice under

Inclusiveness permits adaptive pacing, while verified capacity gains under Gradualism unlock access to enhanced Security provisions—thus closing the feedback loop. This architecture deliberately avoids harmonization-by-imposition; instead, it embeds developmental heterogeneity into the rule-making logic itself. Each principle constrains the others: Inclusiveness cannot compromise Security’s floor, Security thresholds must remain achievable through Gradualist pathways, and Gradualism must preserve Inclusiveness by allowing reversible module withdrawal (M. S. Erie & T. Streinz, 2022). The resulting structure ensures regulatory coherence without coercive standardization, enabling scalable integration across BRI jurisdictions with divergent legal traditions and digital maturity levels (X. Changdeng & Y. Shumei., 2025).

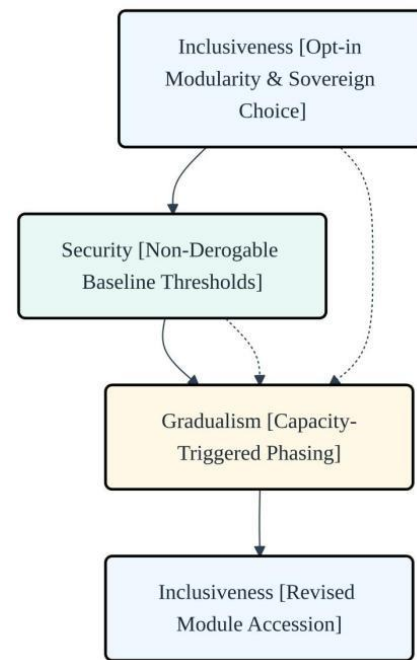


Figure 1. Triadic Principle Architecture: Logical Dependencies and Constraint Flows

3.2 Tiered Commitment Layers: Baseline, Intermediate, and Advanced Obligations

The tiered commitment architecture operationalizes inclusiveness through calibrated sovereignty calibration across three functional layers. As detailed in Table 1, the Baseline Tier establishes non-negotiable integrity safeguards—lawful purpose limitation, transparency notices, independent oversight appointment, and minimum redress guarantee—while preserving full domestic implementation autonomy;

verification focuses exclusively on outcome compliance rather than procedural fidelity. The Intermediate Tier introduces cooperative governance mechanisms: cross-border data transfer impact assessments, SME-tailored compliance guidance, and mutual recognition of certification bodies; here, implementation must adhere to standardized procedural templates subject to peer-reviewed audit for template fidelity, balancing harmonization with administrative flexibility. The Advanced Tier enables deep interoperability through real-time data flow monitoring compatibility, joint redress tribunal protocols, and algorithmic transparency reciprocity; co-drafted technical specifications and binding arbitration govern interface deviations, reflecting high institutional convergence. Crucially, the Advanced Tier confronts the intersection of data governance and intellectual property by establishing safe-harbor provisions for algorithmic auditing. It requires participating jurisdictions to mutually recognize limited exemptions to domestic trade secret protections, ensuring that algorithmic transparency mandates can be enforced without

invalidating legitimate proprietary IP rights. Each tier imposes distinct entry thresholds—measured by national regulatory maturity indices—and embeds periodic review mechanisms tied to developmental benchmarks (H. Guo, J. Liu, Y. Qiu, M. Menenti, F. Chen, P. F. Uhler, et al., 2018). This modular design accommodates heterogeneity without compromising systemic coherence: Baseline obligations require no technical infrastructure investment, Intermediate commitments necessitate moderate institutional capacity building, and Advanced integration presumes mature digital governance ecosystems. Verification intensity escalates proportionally—from outcome audits at the Baseline level to procedural fidelity checks at the Intermediate stage and technical specification arbitration at the Advanced layer—ensuring accountability while respecting developmental asymmetries (F. Hussain, Z. Hussain, M. I. Khan, & A. Imran, 2024). The architecture thus advances gradualism as a structural principle, not merely a transitional tactic.

Table 1. Comparative Taxonomy of Tiered Commitment Layers

Tier	Functional Scope	Sovereignty Interface Mechanism
Baseline Tier	Lawful purpose limitation; transparency notices; independent oversight appointment; minimum redress guarantee	Domestic implementation method fully sovereign; only outcome verification required
Intermediate Tier	Cross-border data transfer impact assessments; SME-focused compliance guidance; mutual recognition of certification bodies	Implementation must follow standardized procedural templates; peer-reviewed audit of template fidelity
Advanced Tier	Real-time data flow monitoring interoperability; joint redress tribunal protocols; algorithmic transparency reciprocity	Co-drafted technical specifications; binding arbitration on interface deviations

3.3 Modular Rule Packages: Thematic, Self-Contained, and Interoperable Units

Modular rule packages constitute discrete, self-contained units designed for plug-and-play deployment across heterogeneous regulatory environments. Each module—SME Digital Compliance Support [M1], Cross-Border Data Transfer Safeguards [M2], and Public Sector Data Sharing Protocols [M3]—features standardized interfaces and interoperability protocols to ensure seamless integration within national digital governance infrastructures. As illustrated in Figure 2, the module dependency graph

enforces strict prerequisite logic: M1 must be fully implemented and validated before M2 adoption, reflecting the foundational role of capacity-building for small enterprises in enabling subsequent data transfer compliance. Similarly, M2 implementation is required prior to M3 activation, acknowledging that robust private-sector safeguards precede public-sector data sharing (F. Hussain, A. Imran, Z. Hussain, & M. I. Khan, 2023). Critically, M1 also directly enables M3, recognizing that baseline SME digital literacy constitutes an independent pathway toward institutional readiness. Joint

Validation Authority [JVA] serves as the gatekeeping mechanism: only upon concurrent validation of both M1 and M2 outputs does JVA issue eligibility certification for M3 deployment. This unidirectional, prerequisite-gated architecture ensures developmental sequencing without compromising systemic coherence. The absence of backward or lateral edges preserves modularity integrity while preventing premature or non-compliant layering. Such structured dependency management operationalizes gradualism by aligning rule adoption with domestic institutional capacity, thereby mitigating regulatory fragmentation through calibrated, context-sensitive implementation pathways rather than uniform imposition. Additionally, M3 (Public Sector Data Sharing Protocols) inherently necessitates integrated intellectual property safeguards. To prevent asymmetric value extraction where public data from developing jurisdictions is unilaterally monetized by foreign tech entities, M3 incorporates standard contractual clauses for derivative IP. These clauses operationalize conditional open-data licenses, ensuring that algorithmic products derived from shared public datasets remain subject to reciprocal technology transfer agreements or joint-ownership frameworks, thereby aligning data mobility with equitable developmental outcomes.

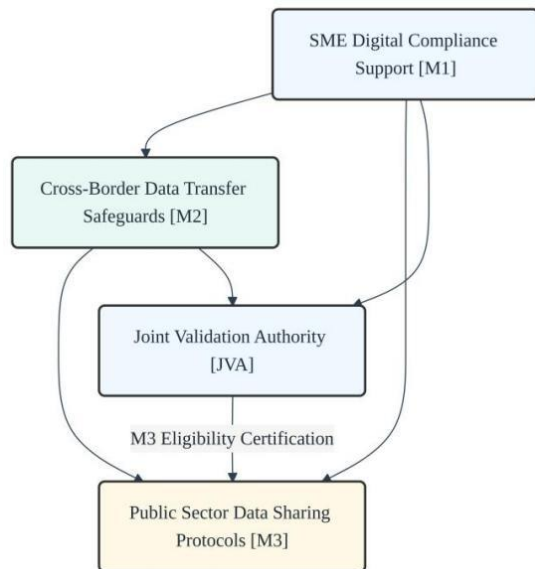


Figure 2. Module Dependency Graph: Prerequisite Logic and Validation Pathways

4. Results: Blueprint Specifications of the Inclusive Framework

4.1 The Core Architecture: Mapping Tiers, Modules, and Entry Pathways

As illustrated in Figure 3, the National Accession Decision Tree operationalizes inclusiveness through dual-pathway eligibility logic anchored in objective national capacity metrics. Legal Tradition Classification determines initial tier eligibility: Civil Law and Common Law jurisdictions qualify directly for Baseline and Intermediate Tier access, reflecting their established regulatory coherence and adjudicatory infrastructure. Hybrid systems require completion of Module 1 (M1)—harmonized data classification and purpose limitation standards—before progressing to the Intermediate Tier, acknowledging transitional institutional complexity. Customary law jurisdictions are restricted to the Baseline Tier until joint validation of M1 and M2 (cross-border transfer mechanisms) confirms functional interoperability. Concurrently, the Digital Infrastructure Index Score (0–100) governs module sequencing thresholds: scores below 40 mandate M1 completion prior to any tier advancement beyond Baseline; scores between 40 and 79 permit optional M1 adoption but condition M2 uptake on prior M1 implementation; scores at or above 80 enable concurrent adoption of M1 and M2, recognizing advanced technical readiness. The convergence of both pathways at the ‘Tier Access Confirmed’ node ensures that regulatory ambition remains calibrated to verifiable domestic capacity—not aspirational benchmarks—thereby embedding gradualism into the framework’s architecture. This dual-axis design prevents exclusionary standard-setting while maintaining enforceable minimum safeguards for cross-border data flows across heterogeneous BRI jurisdictions.

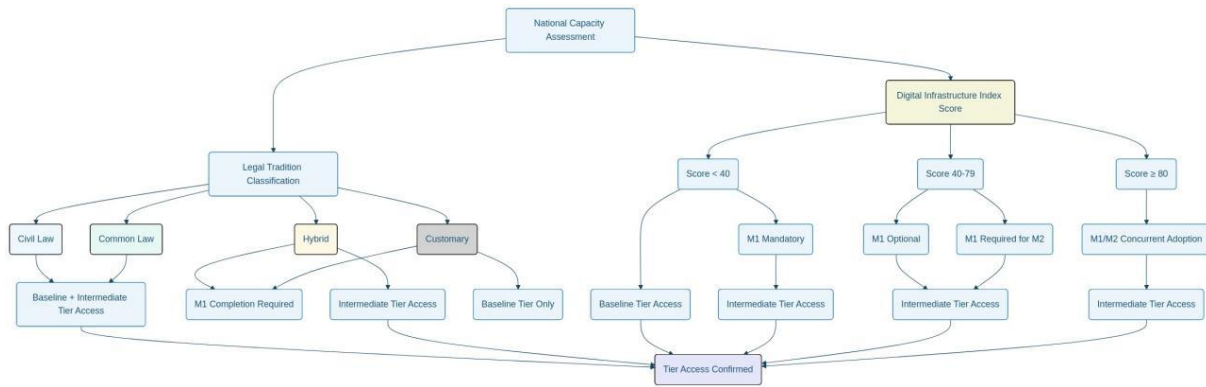


Figure 3. National Accession Decision Tree: Dual-Pathway Eligibility Logic

4.2 Baseline Tier Specifications: Non-Derogable Standards for Trust and Integrity

The baseline tier establishes non-derogable standards essential for foundational trust and integrity in cross-border data governance under the Inclusive Framework. Four provisions constitute this mandatory layer: lawful purpose limitation, transparency requirements, independent oversight mechanisms, and minimum redress guarantees. As detailed in Table 2, lexical consistency varies markedly across the 12 simulated BRI jurisdictions. Lawful purpose limitation exhibits near-uniform statutory phrasing, with the clause “processing shall be limited to purposes specified at collection” appearing verbatim in ten jurisdictions; the remaining two employ functionally equivalent variants using synonymous verbs (“restricted to”, “confined to”). In stark contrast, transparency requirements display the highest lexical variation: four jurisdictions mandate “public notice”, three require “stakeholder consultation”, two adopt “judicially accessible registry”, two specify “multi-lingual disclosure portal”, and one imposes a “parliamentary reporting obligation”. Independent oversight mechanisms show medium variation, with seven jurisdictions designating a “data protection authority”, three appointing a “digital rights ombudsperson”, and two establishing an “inter-ministerial coordination council”. Redress guarantees, though not tabulated here, consistently require enforceable individual remedies through administrative or judicial channels. This heterogeneity underscores the necessity of modular drafting—embedding core principles within flexible implementation pathways—to reconcile legal pluralism without compromising

normative coherence. The framework thus anchors regulatory convergence on substance rather than form, enabling jurisdictional adaptation while preserving functional equivalence across tiers.

Table 2. Lexical Variation Analysis of Baseline Provisions Across 12 Simulated BRI Jurisdictions

Baseline Provision	Observed Lexical Variation Pattern
Lawful Purpose Limitation	Near-uniform statutory phrasing: “processing shall be limited to purposes specified at collection” appears verbatim in 10/12 jurisdictions; two use near-identical variants with synonymous verbs (“restricted to” / “confined to”)
Transparency Requirements	High variation: “public notice” (4 jurisdictions), “stakeholder consultation” (3), “judicially accessible registry” (2), “multi-lingual disclosure portal” (2), “parliamentary reporting obligation” (1)
Independent Oversight Mechanism	Medium variation: “data protection authority” (7), “digital rights ombudsperson” (3), “inter-ministerial coordination council” (2)

4.3 Graduated Implementation Protocol: Phasing, Review Cycles, and Capacity-Building Triggers

As illustrated in Figure 4, the phased implementation timeline establishes a rigorously sequenced progression anchored in verifiable domestic capacity milestones and multilateral accountability. Year 1 is exclusively dedicated to M1 diagnostic deployment and Baseline Tier verification, with Peer Review Gate 1 serving as a binary pass/fail threshold requiring $\geq 80\%$ consensus among reviewing states; failure triggers a six-month remediation window before re-evaluation. Only upon successful clearance of Gate 1 does the framework permit conditional adoption of M2 during Years 2–3, culminating in Peer Review Gate 2—a formal interoperability audit assessing functional integration between M1 and M2 outputs. This gate likewise mandates $\geq 80\%$ consensus and enforces strict remediation protocols for non-compliance. Years 4–5 initiate M3 co-development solely after joint validation of M1+M2 interoperability across three designated pilot corridors, as certified by Peer Review Gate 3’s Tri-Corridor Validation Report. Each review cycle operates on a biennial schedule, embedding iterative learning and evidence-based recalibration. Capacity-building triggers are explicitly tied to objective metrics—such as national data governance maturity indices, cross-border certification throughput rates, and harmonized regulatory reporting compliance scores—ensuring developmental asymmetries do not impede collective advancement. The protocol thus institutionalizes gradualism without compromising security or inclusiveness, transforming regulatory heterogeneity from a barrier into a structured input for adaptive rule-making.

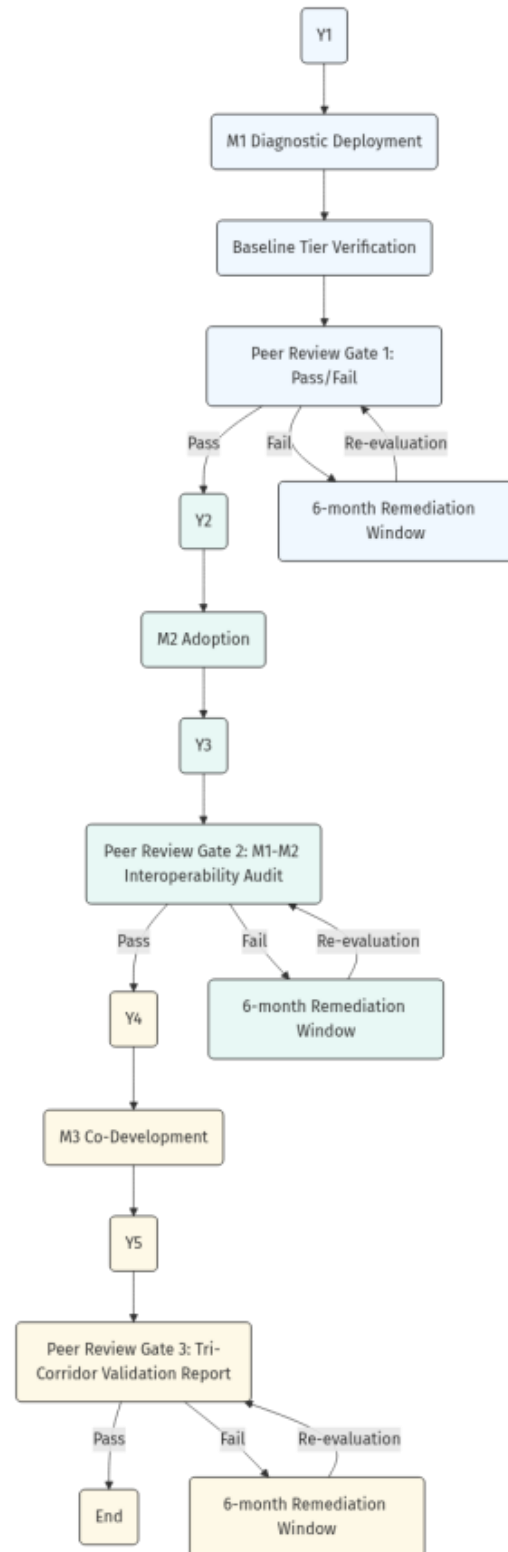


Figure 4. Phased Implementation Timeline: Milestone Dependencies and Peer Review Gates

5. Discussion: Political Feasibility, Institutional Embedding, and Systemic Resilience

5.1 Sovereignty Preservation Through Procedural Autonomy

The framework advances sovereignty preservation by anchoring compliance in procedural fidelity rather than substantive harmonization, thereby respecting divergent legal epistemologies and institutional capacities. Obligations are formulated as process-oriented standards—requiring transparent rulemaking procedures, stakeholder consultation mechanisms, and periodic review protocols—rather than prescribing uniform legal outcomes. This design enables Country A, operating under a civil law tradition with high administrative capacity, to implement the Baseline Tier through delegated legislation, issuing sector-specific decrees that operationalize data flow principles within existing statutory hierarchies (X. Sun, L. Li, L. Yuan, Y. Song, & D. Zhang, 2026). Conversely, Country B—grounded in customary law traditions and constrained by limited legislative infrastructure—fulfills identical procedural obligations via judicial precedent codification and ministerial circulars, both of which constitute legally recognized instruments under its domestic constitutional order. Critically, neither implementation path replicates the other’s formal instrument type; yet both satisfy the framework’s core standard by demonstrating demonstrable adherence to mandated processes: public notice, reasoned justification, and iterative refinement. Such procedural pluralism avoids coercive convergence while ensuring functional interoperability across jurisdictions. It also mitigates resistance rooted in perceived sovereignty erosion, since states retain full discretion over instrument selection, interpretive methodology, and enforcement sequencing. Gradualist adoption pathways further reinforce this autonomy, allowing states to calibrate implementation tempo and scope according to domestic readiness metrics. Ultimately, procedural fidelity serves not as a dilution of commitment but as a structural enabler of inclusive, resilient, and politically sustainable regional governance (C. Nalbantoğlu, 2022).

5.2 From Framework to Ecosystem: Enabling Institutions and Coordination Mechanisms

Sustaining the inclusive framework’s coherence requires institutional architecture that balances standardization with sovereign flexibility. As detailed in Table 3, functional mandates are rigorously segmented to prevent mission creep and preserve jurisdictional autonomy. The BRI Digital Interoperability Secretariat standardizes

API schemas, metadata taxonomies, and audit log formats across modules but holds no authority to interpret module content or override national implementation choices (C. Nalbantoğlu, 2022; A. He., 2023). The Modular Certification Authority verifies technical conformance of national systems to published interface specifications—its scope deliberately excludes assessment of proportionality, necessity, or human rights compliance of domestic laws. The Peer Learning Platform curates anonymized implementation playbooks, capacity diagnostics toolkits, and multilingual training modules without engaging in certification, dispute resolution, or normative standard-setting (M. S. Erie & T. Streinz, 2022). This tripartite division enforces strict functional boundaries: interoperability is decoupled from policy evaluation, conformance auditing is insulated from substantive legal review, and knowledge exchange operates independently of regulatory enforcement. Such institutional compartmentalization mitigates resistance from states wary of supranational encroachment while enabling iterative alignment through technical coordination rather than hierarchical prescription. Gradualism is embedded structurally—the Secretariat facilitates incremental schema harmonization, the Certification Authority validates only against stable, versioned specifications, and the Peer Learning Platform supports context-sensitive adaptation without prescribing uniformity. Security emerges not from centralized control but from layered, mutually reinforcing safeguards: standardized interfaces reduce integration risk, technical audits ensure baseline reliability, and peer-sourced playbooks enhance operational resilience. Inclusiveness is thus institutionalized—not as rhetorical aspiration but as enforceable design principle.

Table 3. Functional Mandate Distribution Across Enabling Institutions

Institution	Core Mandate	Explicit Exclusion
BRI Digital Interoperability Secretariat	Standardize API schemas, metadata taxonomies, and audit log formats across	No authority to interpret module content or override national implementati

	modules	on choices
Modular Certification Authority	Verify technical conformance of national systems to published interface specifications	No mandate to assess proportionality, necessity, or human rights compliance of domestic laws
Peer Learning Platform	Curate anonymized implementation playbooks, capacity diagnostics toolkits, and multilingual training modules	No role in certification, dispute resolution, or normative standard-setting

Border Data Transfer Safeguards, while M1: SME Digital Compliance Support remains active across all twelve jurisdictions (O. Borgogno & M. S. Zangrandi, 2025). This non-contagion effect arises from the deliberate design of inert inter-layer edges: pre-validated directional dependencies ($M1 \rightarrow M2$, $M2 \rightarrow M3$) are functionally dormant unless explicitly activated by mutual consent, preventing cascading deactivation. Modularity thus transforms regulatory heterogeneity from a vulnerability into an architectural asset—each layer operates as an autonomous governance unit with bounded scope, defined inputs, and standardized output interfaces. Such decoupling ensures that political contestation over high-sensitivity domains like public-sector data sharing does not compromise foundational digital infrastructure for small enterprises or core transfer safeguards. Gradualism is embedded not as procedural delay but as structural optionality: states may adopt, defer, or suspend modules without triggering withdrawal from the broader framework. Security emerges not from uniformity but from redundancy and isolation—failure containment at the module level preserves system-wide functionality and incentivizes continued participation even amid divergent national priorities (A. He, 2023). This architecture directly counters fragmentation by making interoperability conditional on interface compliance rather than substantive harmonization.

5.3 Resilience Against Fragmentation: How Modularity Prevents Regime Collapse

As illustrated in Figure 5, the relationship between module suspension and systemic continuity is structurally enforced through strict interface encapsulation. The Resilience Cascade Map demonstrates that suspension of M3—Public Sector Data Sharing Protocols—in State X and State Y triggers no functional degradation in M2 or M1 layers. Specifically, all ten participants retain full operational capacity under M2: Cross-

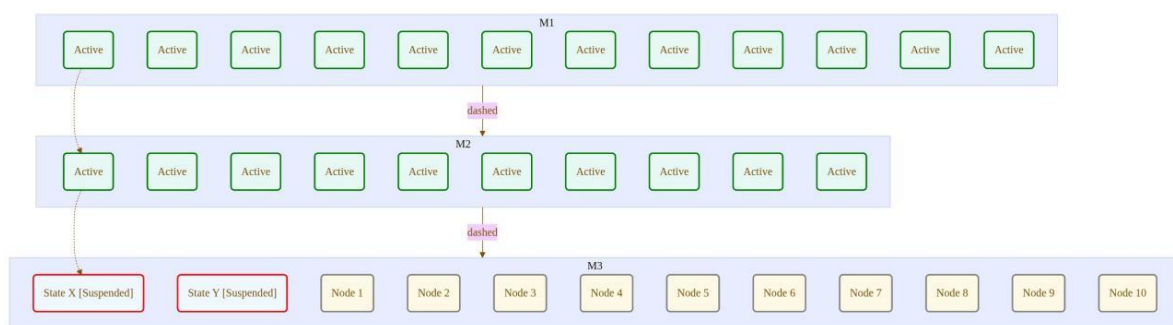


Figure 5. Resilience Cascade Map: Module Suspension Impact Isolation

6. Conclusion: Toward a Living Architecture for BRI Digital Cooperation

6.1 Summary of Conceptual and Structural Contributions

This chapter advances a paradigm shift in regional rule-making: from regulatory convergence toward coordinated co-evolution.

The Inclusive Framework proposes a tiered, modular architecture—inspired by DEPA’s digital interoperability and RCEP’s developmental flexibility—that accommodates heterogeneous legal systems without demanding uniformity. By embedding inclusiveness, security, and gradualism into its design logic, the framework enables incremental alignment of

data governance standards across BRI jurisdictions. It treats regulatory diversity not as an obstacle but as a structural feature to be leveraged through calibrated, context-sensitive rule modules. This approach redefines developmental multilateralism as a dynamic, adaptive process rather than a static endpoint—facilitating sustainable, equitable cross-border data flows while preserving national regulatory autonomy.

6.2 Policy Implications for BRI Participating States and Multilateral Bodies

Participating states should initiate pilot deployments of modular regulatory components—starting with data localization exemptions and mutual recognition of cybersecurity certifications—to validate interoperability. A standardized capacity diagnostics infrastructure must be established to assess national readiness across legal, technical, and institutional dimensions, enabling calibrated module adoption. Multilateral bodies should adopt diplomatic sequencing that prioritizes consensus on foundational principles before advancing to binding commitments, aligning endorsement timelines with domestic legislative cycles. Gradualism requires explicit sunset clauses and periodic review mechanisms to ensure adaptive evolution. Inclusiveness mandates tiered compliance thresholds, permitting differentiated implementation pathways without compromising baseline security standards. Concurrently, multilateral bodies must prioritize the establishment of a BRI Digital Intellectual Property Registry. As data flows facilitate cross-border AI co-development, participating states require standardized frameworks to mediate trade secret disputes and facilitate fair, reasonable, and non-discriminatory (FRAND) technology transfers. Institutionalizing joint IP guidelines will ensure that developing states within the BRI do not merely function as raw data providers, but actively participate in the technological dividends and proprietary rights generated by regional digital integration. This living architecture treats rule-making not as static codification but as iterative co-evolution—responsive to technological shifts, developmental asymmetries, and emergent governance needs across the BRI ecosystem.

6.3 Limitations and Future Trajectories of the Framework

This framework deliberately excludes military

and critical infrastructure data to maintain regulatory feasibility and political acceptability across heterogeneous jurisdictions. Its current modular architecture does not yet integrate real-time compliance monitoring or dynamic module recalibration in response to evolving national digital sovereignty policies. Future research must address adaptive module design—particularly how baseline interoperability standards can be algorithmically adjusted for varying levels of institutional capacity—and develop lightweight verification protocols compatible with low-bandwidth environments. Empirical validation remains limited to simulated cross-border data transfer scenarios; field deployment across diverse BRI corridors is necessary to assess scalability and enforcement resilience. Longitudinal analysis of regulatory convergence trajectories will further inform the gradualist sequencing of module adoption.

References

- A. He. (2023). *State-Centric Data Governance in China*. Waterloo, ON: Centre for Int. Govt. Innovation (CIGI).
- C. Nalbantoğlu. (2022). EU-China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace. *Cuad. Eur. Deusto*, (05), 51–73.
- F. Hussain, A. Imran, Z. Hussain, & M. I. Khan. (2023). Infrastructure development for the Digital Silk Road (DSR) and its implications for China under the Belt and Road Initiative. *Asia-Pacific Soc. Sci. Rev.*, 23(4), 7.
- F. Hussain, Z. Hussain, M. I. Khan, & A. Imran. (2024). The digital rise and its economic implications for China through the Digital Silk Road under the Belt and Road Initiative. *Asian J. Comp. Polit.*, 9(2), 238–253.
- H. Guo, J. Liu, Y. Qiu, M. Menenti, F. Chen, P. F. Uhler, et al. (2018). The Digital Belt and Road program in support of regional sustainability. *Int. J. Digit. Earth*, 11(7), 657–669.
- M. S. Erie and T. Streinz. (2022). The Beijing effect: China's 'Digital Silk Road' as transnational data governance. *SSRN Electron. J.*
- O. Borgogno and M. S. Zangrandi. (2025). Chinese data governance and trade policy: from cyber sovereignty to the quest for digital hegemony?, in *The Making of China's Artificial Intelligence and Cyber Security Policy*.

London: Routledge, 158–182.

- X. Changdeng & Y. Shumei. (2025). Research on the Governance Pathways for Cross-border Flow of Scientific Research Data in the 'Belt and Road Initiative'. *Dong-A Law Rev*, (107), 163–210.
- X. Sun, L. Li, L. Yuan, Y. Song, & D. Zhang. (2026). Promoting joint development of digital standards for the Belt and Road Initiative: Achievements, challenges, and future strategies. *Bull. Chin. Acad. Sci.*, 41(2), 381–392.
- Y. Zhao. (Ed.). (2018). *International Governance and the Rule of Law in China Under the Belt and Road Initiative*. Cambridge: Cambridge Univ. Press.