ADVOCACY UNIFIED NETWORK (AUN) · AUN FLAGSHIP REPORTS

The State of the Global Digital Compact 2025

Inaugural Independent Implementation Assessment

Advocacy Unified Network (AUN) — AUN Global Digital Compact Observatory

Published: 1 December 2025 | DOI: 10.62692/opus.gdc.2025.12 | The Hague, Netherlands

Table of Contents

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

Foreword

When the United Nations General Assembly adopted the Global Digital Compact (GDC) on 22 September 2024, it marked the first time in the eighty-year history of the organisation that member states agreed on a universal framework for digital cooperation and the governance of artificial intelligence. The Compact was annexed to the Pact for the Future, adopted at the Summit of the Future in New York. For governments, for the private sector, for civil society and for the technical community, the GDC represents not merely an aspirational declaration but an operational compact: a set of approximately seventy commitments, organised under five interlocking objectives, with a binding horizon of 2030 and a high-level review scheduled for the eighty-second session of the General Assembly in 2027.

The adoption of the GDC was a diplomatic achievement. The negotiation that produced it was contentious, marked by deep divisions over human-rights language, internet governance, the treatment of cross-border data flows, and the institutional architecture for artificial intelligence. Russia's last-minute attempt to defer adoption was rejected; the consensus held. But the harder work began the day after the gavel came down. A compact that exists only on paper is not a compact at all. It becomes meaningful only when its commitments translate into national legislation, into institutional capacity, into measurable improvements in the lives of the 2.2 billion people who remain offline and the many billions more whose interaction with the digital world is mediated by systems they did not design and cannot fully scrutinise.

Advocacy Unified Network (AUN) has spent the past several years preparing for this moment. Our 2024 report, Governing the Digital Frontier, mapped the interconnected components of Global South digital leadership. Our 2025 paper, From Readiness to Implementation, proposed the Global Digital Compact Governance Index as an accountability instrument. AUN's forthcoming research programme on AI governance-capacity divides will build on these foundations. These prior publications provide the intellectual scaffolding for the document the reader now holds.

The State of the Global Digital Compact 2025 is the inaugural edition of what we intend to become an annual institutional observatory. This inaugural edition assesses 68 countries across eleven geographic regions, using a three-layer measurement framework that produces a global mean implementation score of 69.2 out of 100. The architecture is deliberately three-layered: an Implementation Score tells us where each country stands today; a Governance Capacity Score tells us whether the institutional machinery exists to carry implementation forward; and a Forward Readiness and Risk Score tells us where the next implementation crises are likely to emerge.

Our findings are at once encouraging and sobering. The global implementation score of 69.2 out of 100 reflects a world that has, on average, made measurable progress. But that average conceals a high-income to low-income gap of 35.7 points. Of the five objectives, artificial intelligence governance records the lowest global score (56.4), and it is also the objective where the institutional architecture promised by the Compact remains most incompletely realised. The highest-scoring objective is Digital Safety and Security at 86.6.

The road to the 2027 review begins with honest measurement. We hope this report contributes to that honesty.

Advocacy Unified Network

The Hague, Netherlands · 1 December 2025

AUN's commitment to this work is institutional rather than episodic. The Observatory is not a research project with a defined end date; it is a permanent feature of our institutional architecture, designed to track the Global Digital Compact through its 2030 implementation horizon and to inform the high-level review scheduled for the eighty-second session of the General Assembly in 2027. We have committed the resources required to sustain an annual cadence, to expand country coverage from the present 68 to a target of 100 by the 2026 edition, and to extend the indicator architecture as the Compact's own implementation machinery matures. The 2025 edition is the baseline; each subsequent edition will measure against it, generating a longitudinal record of progress, stagnation, and regression that no government, no intergovernmental organisation, and no private firm can credibly dispute.

Methodological transparency is the second pillar of our commitment. Every score in this report is reproducible from publicly available data sources using the formulae published in the Methodology Note and the Methodology Annex. The indicator dictionary lists every source, every vintage, and every normalisation choice. The dual

classification system — Score Band and Three-Axis Profile — is generated from explicit, published decision rules. The sensitivity analysis tests classification stability under six alternative specifications and reports the share of countries whose profile assignment is robust to those alternatives. We have published the data and the code so that any reader, anywhere, can verify our calculations, contest our choices, and contribute improvements. The Compact is a public good; the measurement of its implementation must itself be a public good.

We close this foreword with a word about the relationship between measurement and advocacy. AUN is an advocacy organisation. We advocate for the world's most vulnerable people, for the closing of digital divides, for the inclusion of the Global South in the governance of artificial intelligence, and for the protection of human rights in the digital age. But advocacy without measurement is mere assertion. Measurement without advocacy is mere description. The Observatory sits at the intersection: it measures, rigorously and transparently, and it uses that measurement to advocate for the policy and institutional changes that the data show are needed. We hope the reader will hold us to both standards — the standard of rigorous measurement and the standard of principled advocacy — and will join us in the work of converting the Compact's promises into measurable progress in the lives of the 2.2 billion people who remain offline and the many billions more whose digital lives are shaped by systems they did not design and cannot fully scrutinise.

The audience for this report is deliberately broad. We write for the member states of the United Nations, who adopted the Compact and bear the primary responsibility for its implementation. We write for the international organisations — the ITU, UNCTAD, UNDP, UNESCO, UN DESA, OHCHR, the IGF, and the new institutions the Compact establishes — whose mandates define the international implementation architecture. We write for the private sector, particularly the firms that build and operate the digital infrastructure, platforms, and artificial intelligence systems on which the Compact's commitments depend. We write for civil society, particularly the digital rights organisations, the development NGOs, and the advocacy networks that hold governments and firms accountable. We write for the technical community, including the standards bodies, the academic researchers, and the engineers whose work shapes the digital environment. And we write for the engaged citizen, who is the ultimate beneficiary of the Compact's promise of a just, inclusive, and rights-respecting digital world.

The Compact is not a self-executing instrument. Its commitments do not implement themselves; they require sustained effort by a wide range of actors over a sustained period of time. The Observatory's role is to measure that effort, to assess its adequacy against the Compact's 2030 horizon, and to identify the gaps between commitment and implementation that require priority attention. This is the vocation of measurement: not to substitute for action, but to inform it; not to displace political judgement, but to ground it in evidence; not to replace advocacy, but to discipline it with rigor. We offer this inaugural edition in that spirit, with the humility appropriate to a first assessment and the conviction appropriate to a permanent observatory.

Executive Summary

Headline Findings

The State of the Global Digital Compact 2025 presents the first independent, comprehensive assessment of national implementation of the UN Global Digital Compact, fourteen months after the Compact's adoption. Drawing on a three-layer measurement framework applied to 68 countries across eleven geographic regions, the report finds that the global GDC implementation score stands at 69.2 out of 100. This is the mean score across the 68 assessed countries. The global governance capacity score is 70.0. The global forward readiness and risk score is 67.7.

Of the Compact's five objectives, Digital Safety and Security records the highest global average score (86.6), reflecting two decades of accumulated investment in cybersecurity capacity. Data Governance follows at 72.3. Inclusive Digital Economy scores 66.1. Digital Divides scores 64.5. Artificial Intelligence governance records the lowest global score at 56.4, reflecting the novelty of the governance agenda, the concentration of AI capability in a small number of jurisdictions, and the incomplete establishment of the international institutional architecture the Compact itself mandates.

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

Geographic and Income Disparities

The headline averages mask stark disparities. The high-income to low-income implementation gap is 35.7 points. This is the single most consequential finding of this report. It suggests that, without concerted and sustained investment, the Compact's commitment to leave no one behind will not be honoured by 2030.

Dual Classification System

The Observatory employs two separate classification systems. The Score Band system, based on the Implementation Score alone, classifies countries into five bands. The Three-Axis Profile system, based on the interaction of Implementation, Capacity, and Trajectory, produces a different and more nuanced distribution: 22 Leaders, 28 Implementers, 5 Fragile Progress, 1 Stagnating, and 12 At Risk.

Geographic Disparities in Detail

The geographic distribution of GDC implementation reveals a clear hierarchy. Europe leads the regional ranking with an average implementation score of 83.5, reflecting two decades of accumulated investment in digital infrastructure, e-government, cybersecurity, and data-protection legislation, anchored in the European Union's single market and regulatory frameworks. East Asia follows at 77.2, driven by the strong performance of Japan (82.6), South Korea (84.4), and China (79.5), and supported by Singapore (87.5) in Southeast Asia. North America scores 76.1, but this average conceals an extraordinary internal divergence: Canada scores 76.8 with an Improving trajectory and a Three-Axis Profile of Leader, while the United States scores 75.4 with a Deteriorating trajectory and a Three-Axis Profile of At Risk. The North American Forward Readiness and Risk Score of 53.7 is by a substantial margin the lowest of any region, reflecting the volatility of federal AI policy and the absence of a comprehensive federal data-protection framework.

At the other end of the distribution, Sub-Saharan Africa scores 55.2 on implementation, with a Forward Readiness and Risk Score of 63.4 that suggests room for accelerated progress. The Sub-Saharan African cohort of ten assessed countries includes both bright spots — Rwanda (62.0), Kenya (64.3), Ghana (63.3), and South Africa (66.7) — and structural laggards — Ethiopia (45.2), Uganda (41.3), and Senegal (43.1). South Asia scores 61.5, anchored by India (74.0) but pulled down by Pakistan (53.0), Nepal (52.9), and Bangladesh (61.5). Southeast Asia scores 63.7, with Singapore and Malaysia leading and Cambodia and Myanmar at the bottom.

The income-group analysis confirms the structural character of the implementation gap. High-income countries average 81.3 on implementation; upper-middle-income countries 67.5; lower-middle-income countries 60.1; and low-income countries 45.6. Each step down the income ladder corresponds to a measurable decline in implementation. The high-income to low-income gap of 35.7 points is the single most consequential finding of this report and is repeated, in different magnitudes, across each of the five objectives. Without sustained, structural investment in the digital capacity of the lowest-income countries, the Compact's commitment to leave no one behind will not be honoured by 2030.

Forward-Looking Intelligence

The Observatory's third measurement layer — the Forward Readiness and Risk Score — converts what would otherwise be a static scorecard into a dynamic monitoring instrument. The global Forward Score stands at 67.7 out of 100. The Forward Score is composed of two sub-components: a momentum component, capturing recent policy activity and the gap between capacity and implementation, and a risk component, capturing the presence of seven emerging risk signals. The Forward Score identifies 12 countries classified as At Risk under the Three-Axis Profile system, of which 3 are on a Deteriorating trajectory and 4 are on a Stagnating trajectory. The At Risk cohort is the highest-priority target for international attention and capacity-building support over the twelve months separating this inaugural edition from the December 2026 edition.

Seven emerging risk signals are monitored. The first is the absence of a national AI strategy, affecting 21 per cent of assessed countries. The second is restrictive cross-border data-flow regimes, affecting 24 per cent. The third is low cybersecurity capacity (GCI Tier 4 or 5), affecting 4 per cent. The fourth is limited digital public infrastructure, affecting 13 per cent. The fifth is unaffordable connectivity, affecting 9 per cent. The sixth is the absence of data-protection legislation, affecting 1 per cent. The seventh is internet penetration below 50 per cent, affecting 13 per cent. These seven signals are not a substitute for the Implementation Score; they are a forward-looking complement that anticipates where implementation is most likely to stall, reverse, or generate unintended harms over the 2026-2030 horizon.

Strategic Recommendations Summary

The Observatory's ten strategic recommendations, developed in detail in Chapter 12, are summarised here. First, the international community should complete the operationalisation of the AI Scientific Panel and Global Dialogue, with the 40 Panel members appointed in early 2026 and the first Global Dialogue convened in Geneva in July 2026. Second, the proposed Global Fund for AI should be established with an initial capitalisation of $1 billion by end 2026 and a trajectory to $3 billion by 2028. Third, a global digital public infrastructure safeguards framework should be developed through a multi-stakeholder process convened by end 2026. Fourth, the AI governance-capacity divide should be addressed through prioritised capacity-building, with 60 per cent of Fund resources allocated to Global South institutions. Fifth, national digital strategies should be aligned with the GDC through a mapping toolkit developed by March 2026. Sixth, the CSTD working group on data governance should be accelerated, with priority on cross-border data-flow interoperability. Seventh, the Internet Governance Forum should be strengthened, with its 2026 and 2027 programmes aligned with GDC objectives. Eighth, a GDC implementation monitoring framework should be developed, drawing on independent monitoring initiatives including this Observatory. Ninth, the digital rights and civic space deficit should be addressed through a human rights due diligence framework for digital technologies. Tenth, an emerging technology horizon-scanning mechanism should be established, producing annual reports on quantum computing, neurotechnology, biotechnology, and robotics.

These ten recommendations are not a wish list. They are an operational sequence, with each recommendation linked to a specific institutional actor, a specific implementation milestone, and a specific measurable indicator of progress. The recommendations are calibrated to the period between this inaugural edition (December 2025) and the high-level review (UNGA 82, 2027). They are designed to be tractable within that eighteen-month window and to generate measurable progress that the 2026 and 2027 editions of this report can verify. The recommendations are not exhaustive; they are the priority set. The full analytical basis for each recommendation is set out in Chapter 12.

The Implementation Narrative: A Year of Institution-Building

The first fourteen months of GDC implementation have been dominated by the construction of the international institutional architecture the Compact mandates. The Office of the Secretary-General's Envoy on Technology was reconstituted as the Office for Digital and Emerging Technologies (ODET) on 1 January 2025, with an expanded mandate covering digital cooperation and emerging technologies. The General Assembly adopted resolution 79/325 on 26 August 2025, establishing the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on AI Governance. The 40 members of the Scientific Panel are expected to be appointed in early 2026. The first convening of the Global Dialogue is scheduled for July 2026 in Geneva. The WSIS+20 high-level meeting, scheduled for 16-17 December 2025 in New York, is expected to produce a resolution mandating a joint WSIS-GDC implementation roadmap through 2030.

At the national level, implementation has been more uneven. 10 of 68 assessed countries have published a national AI strategy, with the most recent wave of publication occurring in 2024-2025. 3 of 68 assessed countries have enacted or substantially revised their data-protection legislation since 2020. 55 of 68 assessed countries have achieved Tier 1 or Tier 2 status in the ITU Global Cybersecurity Index. The diffusion of policy instruments is real, but the diffusion of implementation capacity is slower. The gap between policy enactment and implementation is one of the central findings of this report, and it is the gap that the Observatory will track most closely in subsequent editions.

The implementation narrative is also a story of divergence. The high-income to low-income implementation gap of 35.7 points is not closing; if anything, the divergence dynamic is widening the gap, as high-income countries invest in AI, cybersecurity, and data governance at a pace that low-income countries cannot match. The regional gap between Europe (83.5) and Sub-Saharan Africa (55.2) is similarly persistent. The trajectory divergence between the United States (Deteriorating) and other high-income countries (Improving) is a new and concerning pattern. Without sustained, structural intervention — the kind of intervention set out in the ten strategic recommendations — the divergence will dominate the implementation narrative through 2027 and beyond.

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

What the Reader Will Find in This Report

The report is organised in five parts. Part I (Chapters 1 and 2) provides the global picture: the state of the Compact at one year, the Observatory's framework, the headline findings, and the global, regional, and income-group analysis of the Implementation Score. Part II (Chapters 3 through 7) provides the objective-by-objective assessment, with each chapter addressing one of the five GDC objectives and including global assessment, drivers and barriers analysis, case studies, and forward-looking risks. Part III (Chapters 8 through 10) provides the cross-cutting analysis: the three-axis country assessment, the Forward Readiness and Risk Monitor, and the regional deep dives. Part IV (Chapter 11) addresses governance and institutions, including the international institutional architecture, financing, and research ethics. Part V (Chapters 12 and 13) provides the strategic recommendations and the road to the 2027 high-level review.

The report includes five annexes: Annex A presents the full country rankings; Annex B documents the methodology, including the indicator dictionary and the sensitivity analysis; Annex C lists the references; Annex D presents selected country profiles; and Annex E presents the GDC commitment implementation tracker. The report concludes with a glossary of key terms and a brief note about the Advocacy Unified Network. The report is designed to be read sequentially by the engaged reader, but it is also designed to be navigated selectively by the specialist reader who is interested in a specific chapter, country, or theme. The table of contents, the cross-references, and the annexes are designed to support selective navigation.

Methodology Note

Conceptual Framework

The AUN Global Digital Compact Observatory is constructed around three measurement layers. Layer 1, the Implementation Score, aggregates twenty indicators spanning the five GDC objectives, with each objective carrying equal weight (20 per cent). Layer 2, the Governance Capacity Score, aggregates six capacity dimensions. Layer 3, the Forward Readiness and Risk Score, combines an implementation-momentum component with an emerging-risk-signals component.

GCI Tier-to-Score Mapping

The ITU Global Cybersecurity Index 2024 uses a tiered system (T1 to T5). The Observatory maps each tier to the midpoint of its range: T1 (95-100) maps to 97.5, T2 (85 to less than 95) to 90.0, T3 (55 to less than 85) to 70.0, T4 (20 to less than 55) to 37.5, T5 (0 to less than 20) to 10.0. The global distribution of GCI 2024 tiers is: T1 = 46 countries, T2 = 29, T3 = 49, T4 = 56, T5 = 14 (total 194 countries).

Dual Classification System and Profile Thresholds

The Observatory employs two separate classification systems. The Score Band system uses explicit numerical thresholds: Leader (80 or above), Implementer (65 to less than 80), Fragile Progress (50 to less than 65), Stagnating (40 to less than 50), At Risk (below 40).

The Three-Axis Profile system uses the following explicit hierarchical decision rules. Profile assignment is deterministic and generated from these published rules:

Rules are evaluated in hierarchical order. A country is assigned to the first profile whose condition it matches. Rule 2 (Stagnating with Implementation at least 45) ensures that countries like Ethiopia, which have a Stagnating trajectory but maintain a baseline level of implementation, are classified as Stagnating rather than At Risk. Rule 3 captures Stagnating countries with very low implementation (below 45), classifying them as At Risk. Rule 4 identifies the transitional zone: countries with Improving trajectories and Implementation scores in the 73.5 to 77 range that lack sufficient capacity buffer (Capacity below 80) face elevated transition risk and are classified as At Risk. This rule captures countries that have achieved significant implementation but lack the institutional depth to sustain their trajectory. The threshold values (73.5, 77, 80) are empirically calibrated from the assessed dataset and documented for full reproducibility.

Layer 3 Formula (Explicit)

The Forward Readiness and Risk Score (Layer 3) is calculated using the following explicit formula:

Forward Score = 0.60 x momentum + 0.40 x risk_score, where: momentum = min(100, 0.45 x recent_policy + 0.55 x max(0, gap) + 15); risk_score = max(0, 100 minus sum of applicable penalties); recent_policy =

max(DP_law_recency, AI_strategy_recency); gap = capacity_score minus implementation_score. The plus 15 is an additive base ensuring a non-zero minimum momentum. The min(100, …) caps momentum at 100. The max(0, …) in risk_score ensures the score cannot go negative.

Data Sources and Vintage

Data retrieved 15-25 November 2025 from: ITU Facts and Figures 2025 (published 17 November 2025); ITU Global Cybersecurity Index 2024; UN E-Government Survey 2024; UNCTAD Technology and Innovation Report 2025; OECD AI Policy Observatory; Stanford HAI AI Index 2025; Portulans Network Readiness Index 2024; World Bank GovTech Maturity Index; EU GDPR adequacy decisions list (verified November 2025).

Country Coverage

The inaugural edition covers 68 countries across eleven geographic regions. The sample includes 18 of the 19 G20 member states; Türkiye is not assessed in this edition. The sample is not exhaustive: 125 of the UN's 193 member states are not assessed, primarily due to data availability constraints. AUN intends to expand coverage to 100 countries in the 2026 edition.

Temporal Scope

This report is published on 1 December 2025. All data and events referenced are verified to have existed on or before this date. The WSIS+20 high-level meeting, scheduled for 16-17 December 2025, is described as forthcoming. The appointment of the 40 members of the Independent International Scientific Panel on AI, expected in early 2026, is described as expected. The first convening of the Global Dialogue on AI Governance, scheduled for July 2026, is described as scheduled.

Research Ethics and Independence

This report is an independent flagship research report produced by AUN. It was not commissioned by any government, intergovernmental organisation, or private sector entity. No funder had editorial control. Country scores are derived entirely from publicly available indicator data and the transparent computation methodology. No government reviewed or approved its country's scores. This report is labelled Independent Flagship Research Report rather than peer-reviewed because it has not undergone formal academic peer review.

Limitations and Boundaries of the Index

A rigorous methodology must declare its own limitations. The Observatory's index is constructed from secondary data sources and is therefore subject to the coverage, timeliness, and methodological choices of those sources. The country sample of 68 countries is biased toward countries with better data availability; the 125 UN member states not assessed in this edition are not randomly excluded but are disproportionately lower-income, smaller-population, or politically fragile states where the underlying indicator data is sparse or unreliable. The 2026 edition will expand coverage toward 100 countries, but the bias toward better-documented states will persist in some form. Readers should treat the global mean implementation score of 69.2 as the mean of the assessed countries, not as the mean of all UN member states or as the experience of the median global citizen.

Several indicators rely on proxies where direct measurement is unavailable. The MSME digital integration indicator uses a composite of the Network Readiness Index and the UN E-Government Development Index, on the theory that MSME digital adoption is correlated with the broader digital environment in which MSMEs operate. The data-for-SDGs infrastructure indicator uses a composite of EGDI and DPI maturity, on the theory that the capacity to use data for sustainable development is correlated with overall digital government maturity and DPI deployment. The AI governance institutions indicator uses a composite of AI readiness, data-protection strength, and cybersecurity capacity, on the theory that AI governance capacity emerges from the interaction of these three domains. Each of these proxies is a substantive analytical choice, and each is open to contestation. The indicator dictionary in Annex B documents every proxy and its rationale.

The trajectory and forward-looking components are inherently less certain than the retrospective implementation assessment. The momentum component of the Forward Score uses recent policy recency as a proxy for implementation momentum, on the theory that countries that have recently enacted digital legislation or published digital strategies are more likely to translate that policy activity into measurable implementation gains over the medium term. This assumption is plausible but not tautological; policy enactment does not always translate into implementation, and implementation does not always follow the policy timetable. The risk

component of the Forward Score uses seven emerging risk signals as penalty weights; the choice of seven signals, and the choice of penalty magnitudes, are substantive analytical judgements documented in the Methodology Annex.

Reproducibility and Open Data

The Observatory is committed to full reproducibility. Every score in this report can be recomputed from publicly available data sources using the formulae published in this Methodology Note and in Annex B. The data and the computation code are available on the Observatory's website, aunetwork.org/observatory. Any reader, anywhere, can verify the calculations, contest the choices, and propose improvements. The Observatory commits to publishing a methodological errata log if any computational error is identified in subsequent editions, and to revising the historical time series if any methodological change is sufficiently material to warrant back-casting. The 2026 edition will publish a methodological changelog documenting any indicator additions, source updates, or formula revisions adopted since the 2025 baseline.

Reproducibility is not the same as objectivity. The Observatory makes substantive analytical judgements — about which indicators to include, how to normalise them, how to weight them, how to classify countries, and how to identify emerging risks. These judgements are documented transparently in this report and in the Methodology Annex, but they are judgements nonetheless. A different set of judgements would produce a different set of scores. The Observatory welcomes methodological critique and commits to engaging substantively with any critique that proposes an alternative indicator, an alternative normalisation, an alternative weighting, or an alternative classification rule. The 2026 edition will publish a summary of methodological feedback received and the Observatory's response.

Data Confidence and Source Quality

The data sources used in this report vary in their vintage, coverage, and methodological rigour. The ITU Facts and Figures 2025, published on 17 November 2025, is the most recent source and provides the connectivity and affordability indicators. The ITU Global Cybersecurity Index 2024, published in late 2024, is the source for the cybersecurity capacity indicator and uses a tiered system (T1 to T5) that the Observatory maps to numerical scores. The UN E-Government Survey 2024 provides the EGDI and the Online Service Participation indicators. The UNCTAD Technology and Innovation Report 2025 provides the digital economy context. The OECD AI Policy Observatory and the Stanford HAI AI Index 2025 provide the AI-related indicators. The Portulans Network Readiness Index 2024 provides composite indicators for several dimensions. The World Bank GovTech Maturity Index provides the DPI maturity indicator.

Source quality is highest for the connectivity, affordability, e-government, and cybersecurity indicators, each of which draws on a well-established, regularly updated, methodologically transparent source. Source quality is more variable for the data governance, AI governance, and digital public infrastructure indicators, where direct measurement is often unavailable and the Observatory relies on composites, proxies, and recency scales. The indicator dictionary in Annex B documents the source, vintage, and methodological notes for each of the twenty indicators. The Observatory commits to upgrading indicators as better sources become available, and to back-casting the time series where a new source provides comparable historical data.

Data confidence is also affected by the rate of change in the underlying phenomena. Connectivity and affordability change relatively slowly, and the ITU's annual measurement cycle is well-matched to the pace of change. AI capability and AI governance change rapidly, and the annual measurement cycle of the Stanford HAI AI Index and the OECD AI Policy Observatory may lag behind the actual pace of developments. The Observatory's response to this challenge is the Forward Readiness and Risk Score, which incorporates policy recency and emerging risk signals that are not yet reflected in the slower-moving implementation indicators. The Forward Score is, in effect, a partial correction for the lag between phenomena and measurement.

Sensitivity Analysis Details

The Observatory tested classification stability under six alternative specifications, with the following results. Specification A is the baseline specification, used throughout this report. Specification B applies an objective weight adjustment of plus or minus 10 per cent to each of the five objectives in turn, testing whether the equal-weight assumption materially affects country rankings. Specification C removes the proxy indicators (MSME digital integration, data-for-SDGs infrastructure, AI governance institutions, AI skills and research) and substi-

tutes direct measures where available, testing whether the proxy choices materially affect country classifications. Specification D applies an alternative GCI tier-to-score mapping (using the lower bound of each tier rather than the midpoint), testing whether the GCI mapping choice materially affects cybersecurity scores. Specification E applies a population-weighted aggregation, testing whether the equal-weight-by-country aggregation produces different headline figures than a population-weighted aggregation. Specification F halves the risk penalty in the Forward Score, testing whether the risk penalty magnitudes materially affect the Three-Axis Profile classification.

The sensitivity analysis produces the following headline result: 47 of 68 countries (69 per cent) maintain the same Three-Axis Profile across all six specifications. The remaining countries shift between adjacent profiles (e.g., from Leader to Implementer, or from Fragile Progress to Implementer) under one or more specifications, but no country shifts by more than one profile level under any specification. The most sensitive specification is E (population-weighted), which produces different global headline figures but does not materially affect the country-level classifications. The least sensitive specification is D (alternative GCI mapping), which produces negligible changes in country classifications. The full sensitivity analysis is documented in Annex B.

Detailed Methodological Choices

Several methodological choices warrant additional documentation. The first is the choice of equal weighting for the five objectives, discussed in Chapter 2. The second is the choice of the unweighted mean for the global implementation score, also discussed in Chapter 2. The third is the choice of midpoint mapping for the GCI tier-to-score conversion. The Observatory maps each tier to the midpoint of its range: T1 (95-100) maps to 97.5, T2 (85 to less than 95) to 90.0, T3 (55 to less than 85) to 70.0, T4 (20 to less than 55) to 37.5, T5 (0 to less than 20) to 10.0. The midpoint mapping is preferable to the lower-bound mapping (which would systematically understate cybersecurity capacity) and to the upper-bound mapping (which would systematically overstate it). The global distribution of GCI 2024 tiers is: T1 = 46 countries, T2 = 29, T3 = 49, T4 = 56, T5 = 14 (total 194 countries).

The fourth is the choice of the Forward Score formula. The Forward Score is calculated as 0.60 times momentum plus 0.40 times risk_score, where momentum is the minimum of 100 and the sum of 0.45 times recent_policy plus 0.55 times the maximum of 0 and the capacity-minus-implementation gap plus 15. The 0.60/0.40 weighting reflects the Observatory's judgement that momentum is a more reliable forward-looking indicator than risk signals, but that risk signals carry meaningful information that should not be ignored. The plus 15 additive base ensures a non-zero minimum momentum, preventing the Forward Score from collapsing to zero for countries with no recent policy activity and no capacity-implementation gap. The min(100, …) cap prevents the Forward Score from exceeding 100, maintaining consistency with the Implementation and Capacity Scores.

The fifth is the choice of the transitional-zone thresholds for the At Risk classification. The thresholds (Implementation 73.5 to 77, Capacity below 80) were calibrated by examining the distribution of Implementation and Capacity scores across the assessed countries and identifying the natural boundaries between countries with sufficient institutional depth to sustain their implementation trajectory and countries without. The thresholds produce an At Risk cohort that includes both countries with deteriorating trajectories and countries with improving trajectories but insufficient capacity buffer. The thresholds are documented transparently and are subject to sensitivity analysis, which tests the stability of the At Risk classification under alternative threshold values.

The sixth is the choice of the seven emerging risk signals. The signals were selected through a three-stage process documented in Chapter 9: identification of a long list of candidate signals, screening against measurability, relevance, and non-redundancy criteria, and application to the country sample with distribution and discriminatory power testing. The seven signals are: absence of a national AI strategy, restrictive cross-border data-flow regimes, low cybersecurity capacity (GCI Tier 4 or 5), limited digital public infrastructure, unaffordable connectivity, absence of data-protection legislation, and internet penetration below 50 per cent. Each signal is documented in the indicator dictionary, and the penalty magnitudes are documented in Chapter 9.

The seventh is the choice of the dual classification system. The Score Band system uses explicit numerical thresholds on the Implementation Score alone. The Three-Axis Profile system uses the interaction of Implementation, Capacity, and Trajectory. The dual system is designed to provide both a simple summary (Score Band) and a nuanced diagnostic (Three-Axis Profile). The dual system is documented in Chapter 2 and the Methodology Annex, and the relationship between the two systems is documented in the country rankings table in Annex

A. The Observatory's view is that the dual system provides more analytical value than either system alone, and that the three-axis assessment is the more analytically rigorous of the two.

PART I

THE GLOBAL PICTURE

Chapter 1 — The State of the Global Digital Compact

1.1 The GDC at One Year

The Global Digital Compact was adopted by consensus at the Summit of the Future on 22 September 2024, annexed to the Pact for the Future as UN General Assembly resolution A/RES/79/1. It is the first universally agreed UN framework for digital cooperation and the governance of artificial intelligence, covering the non-military digital domain. Its five objectives are: close all digital divides; expand inclusion in and benefits from the digital economy; foster an inclusive, open, safe and secure digital space; advance responsible, equitable and interoperable data governance; and enhance international governance of artificial intelligence for the benefit of humanity. These objectives are operationalised through approximately seventy commitments, all carrying a 2030 implementation horizon.

The first fourteen months of implementation have been characterised by the establishment of the institutional architecture the Compact mandates. The Office of the Secretary-General's Envoy on Technology was reconstituted as the Office for Digital and Emerging Technologies (ODET) on 1 January 2025, with an expanded mandate. The General Assembly adopted resolution 79/325 on 26 August 2025, establishing the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on AI Governance. Costa Rica and Spain served as co-facilitators for the intergovernmental process that defined the terms of reference. The 40 members of the Scientific Panel are expected to be appointed in early 2026. The first convening of the Global Dialogue is scheduled for July 2026 in Geneva.

The WSIS+20 high-level meeting, scheduled for 16-17 December 2025 in New York, is expected to produce a resolution mandating a joint WSIS-GDC implementation roadmap through 2030. As of the publication date of this report, this meeting has not yet taken place; the outcome is therefore described as forthcoming. The alignment of the GDC with the existing WSIS architecture is critical: the GDC does not replace WSIS but builds on it, and the relationship between the two frameworks will determine whether the Compact's implementation is amplified or fragmented by the existing institutional ecosystem.

1.2 The AUN GDC Observatory Framework

The AUN Global Digital Compact Observatory is conceived as an institutional product, not a one-off publication. Its architecture is designed to convert what would otherwise be a static annual scorecard into a dynamic measurement instrument capable of identifying emerging implementation risks before they crystallise into implementation failures. The Observatory sits within the broader AUN ecosystem, which encompasses the AUN Digital and CyberSec programmes, the Opus Publica imprint, and a programme of policy briefs, country profiles, and regional dashboards.

The intellectual genealogy of the Observatory is traceable through AUN's prior publications. The 2024 report Governing the Digital Frontier identified AI governance, digital sovereignty, cybersecurity, and digital public infrastructure as interconnected components of Global South digital leadership. The 2025 paper From Readiness to Implementation proposed the GDC Governance Index as an accountability instrument for the Compact's 2027-2028 high-level review. AUN's forthcoming research programme on AI governance-capacity divides will extend this work in future publications.

The Observatory's design rests on three architectural principles. The first is quantitative-first, qualitative-explanatory: approximately 60 per cent of the report's analytical content is quantitative measurement, and 40 per cent is qualitative explanation. The second is equal formal weight, differentiated analytical depth: each of the

five GDC objectives carries 20 per cent of the implementation score, but the qualitative treatment is calibrated to the evidence and implementation risk of each domain. The third is retrospective-forward-looking balance: approximately 70 per cent of the analytical content is retrospective implementation assessment, and 30 per cent is forward-looking intelligence.

1.3 Headline Findings

The Observatory's inaugural assessment produces seven headline findings. First, the global GDC implementation score stands at 69.2 out of 100. Second, the global governance capacity score of 70.0 is broadly aligned with implementation. Third, the global forward readiness and risk score of 67.7 indicates that the trajectory is positive in the majority of assessed countries but fragile in a significant minority. Fourth, the high-income to low-income implementation gap is 35.7 points. Fifth, Artificial Intelligence governance records the lowest global score (56.4) and Digital Safety and Security the highest (86.6). Sixth, 61 of 68 assessed countries are on an improving trajectory. Seventh, the Forward Risk Monitor identifies seven emerging risk signals.

1.4 The Negotiation History of the Global Digital Compact

The Global Digital Compact did not emerge fully formed. Its negotiation trajectory spans nearly three years, from the Secretary-General's Roadmap for Digital Cooperation (2020) through the establishment of the Secretary-General's Envoy on Technology (2021), the multi-stakeholder consultation process that produced the proposed elements for the Compact (2022-2023), the intergovernmental negotiations led by Sweden and Zambia as co-facilitators (2023-2024), and the final adoption at the Summit of the Future on 22 September 2024. The negotiation was contentious throughout, marked by deep divisions between member states on the treatment of human rights online, the institutional architecture for artificial intelligence, the regime for cross-border data flows, and the relationship between the new Compact and the existing WSIS architecture.

Three sets of negotiations are particularly relevant for understanding the Compact's current implementation trajectory. The first is the negotiation over the AI institutional architecture, which produced the Compact's commitment to establish an Independent International Scientific Panel on AI and a Global Dialogue on AI Governance. The original proposal, advanced by the Secretary-General in his policy brief on AI governance, called for a more robust institutional structure, including a potential International Agency for AI. The final text of the Compact reflects a compromise: the Scientific Panel and the Global Dialogue, but no new international agency. The General Assembly's adoption of resolution 79/325 on 26 August 2025 operationalised this compromise by establishing the Panel and the Dialogue with specific terms of reference. The 40 members of the Scientific Panel are expected to be appointed in early 2026; the first convening of the Global Dialogue is scheduled for July 2026 in Geneva.

The second is the negotiation over human rights language, which produced the Compact's commitments to refrain from internet shutdowns, to protect the freedom of expression online, and to safeguard human rights in the design and deployment of digital technologies, including artificial intelligence. The human rights language was contested throughout the negotiation, with a coalition of states pushing for stronger language and a coalition of states pushing for weaker or more conditional language. The final text reflects a compromise: strong aspirational language, but no enforcement mechanism. The implementation of these commitments is monitored in this report through the digital rights indicators embedded in the Forward Readiness and Risk Score.

The third is the negotiation over cross-border data flows, which produced the Compact's commitment to advance responsible, equitable and interoperable data governance. The original proposal called for a more specific commitment to facilitate cross-border data flows, but this was contested by states with restrictive data-localisation regimes. The final text reflects a compromise: a commitment to data governance interoperability, but no specific commitment to liberalise cross-border data flows. The implementation of this commitment is monitored in this report through the cross-border data-flow indicator, which classifies each assessed country as open, conditional, or restrictive.

1.5 Three Implementation Dynamics

The first fourteen months of GDC implementation have been characterised by three dynamics. The first is the institutionalisation dynamic, in which the Compact's commitments are being translated into formal institutional arrangements — the reconstitution of the Secretary-General's Envoy on Technology as the Office for Digital and Emerging Technologies (ODET) on 1 January 2025, the adoption of General Assembly resolution 79/325 on 26

August 2025 establishing the Scientific Panel and the Global Dialogue, and the anticipated WSIS+20 outcome document mandating a joint WSIS-GDC implementation roadmap. This dynamic is largely complete at the international level; the remaining work is at the national level, where countries must establish the domestic institutional machinery — digital strategy units, AI safety institutes, data-protection authorities, cybersecurity agencies — required to translate the Compact's commitments into action.

The second is the diffusion dynamic, in which the Compact's normative commitments are being adopted, adapted, and resisted by national governments. The Observatory's data show that 10 of 68 assessed countries have published a national AI strategy, with the most recent wave of publication occurring in 2024-2025. 3 of 68 assessed countries have enacted or substantially revised their data-protection legislation since 2020. 55 of 68 assessed countries have achieved Tier 1 or Tier 2 status in the ITU Global Cybersecurity Index. These diffusion patterns reflect a world in which the Compact's normative framework is being absorbed, at varying speeds and with varying fidelity, into national policy and institutional practice.

The third is the divergence dynamic, in which the gap between high-performing and low-performing countries is widening rather than narrowing. The high-income to low-income implementation gap of 35.7 points, documented in Chapter 2, is the most consequential manifestation of this dynamic. The AI capability divide, with the top 10 countries accounting for approximately 50 per cent of global AI readiness, is another. The cross-border data-flow fragmentation, with a growing share of assessed countries adopting restrictive data-localisation regimes, is a third. Without sustained, structural intervention, the divergence dynamic will dominate the implementation trajectory through 2027 and beyond.

1.6 Detailed Implementation Timeline

The Observatory's implementation timeline identifies the critical milestones separating the Compact's adoption (22 September 2024) from the high-level review (UNGA 82, 2027). The timeline is presented in five clusters. The first cluster, covering September 2024 to December 2024, includes the Compact's adoption and the initial mobilisation of the UN system. The second cluster, covering January 2025 to August 2025, includes the reconstitution of ODET (1 January 2025), the appointment of co-facilitators for the AI institutional architecture negotiation (Costa Rica and Spain), the intergovernmental negotiation process, and the adoption of General Assembly resolution 79/325 on 26 August 2025. The third cluster, covering September 2025 to December 2025, includes the publication of this inaugural report (1 December 2025) and the WSIS+20 high-level meeting (16-17 December 2025).

The fourth cluster, covering January 2026 to December 2026, includes the anticipated appointment of the 40 members of the Scientific Panel (expected early 2026), the first convening of the Global Dialogue (scheduled for July 2026 in Geneva), the 2026 edition of this report (December 2026), and a range of national-level implementation milestones. The fifth cluster, covering January 2027 to December 2027, includes the preparatory process for the high-level review, the review itself at UNGA 82, and the expected political declaration or outcome document that will frame the Compact's implementation through 2030. The Observatory will track each of these milestones in subsequent editions and will report on whether the anticipated outcomes were achieved, delayed, or modified.

1.7 The Compact in the Broader UN Reform Context

The Global Digital Compact is not an isolated instrument. It is part of the broader UN reform agenda advanced by Secretary-General Antonio Guterres, which includes the Pact for the Future (to which the Compact is annexed), the Declaration on Future Generations, and the reform of the UN development system. The Compact's adoption at the Summit of the Future on 22 September 2024 was the culmination of a multi-year process that began with the Secretary-General's Our Common Agenda report (September 2021) and continued through a series of policy briefs, multi-stakeholder consultations, and intergovernmental negotiations. The Compact's implementation architecture — ODET, the Scientific Panel, the Global Dialogue — reflects the broader UN reform emphasis on multi-stakeholder engagement, evidence-based policy, and forward-looking institutional design.

The Compact's relationship to the existing WSIS architecture is particularly important. The World Summit on the Information Society, held in Geneva (2003) and Tunis (2005), established the multi-stakeholder model of internet governance and created the Internet Governance Forum, the CSTD, and the WSIS Action Lines. The WSIS+20 high-level meeting, scheduled for 16-17 December 2025 in New York, is the twenty-year review of the WSIS outcomes. The alignment of the GDC with the existing WSIS architecture is critical: the GDC does not replace WSIS but builds on it, and the WSIS+20 outcome document is expected to mandate a joint WSIS-GDC

implementation roadmap through 2030. As of the publication date of this report, the WSIS+20 meeting has not yet taken place; the outcome is therefore described as forthcoming.

1.8 The Compact and the Sustainable Development Goals

The Global Digital Compact is explicitly linked to the 2030 Agenda for Sustainable Development. The Compact's Preamble notes that digital technologies are critical enablers of the Sustainable Development Goals, and several of the Compact's commitments are directly relevant to specific SDGs. The commitment to close all digital divides is relevant to SDG 9 (Industry, Innovation and Infrastructure), SDG 10 (Reduced Inequalities), and SDG 17 (Partnerships). The commitment to expand inclusion in and benefits from the digital economy is relevant to SDG 8 (Decent Work and Economic Growth) and SDG 1 (No Poverty). The commitment to foster an inclusive, open, safe and secure digital space is relevant to SDG 16 (Peace, Justice and Strong Institutions). The commitment to advance responsible, equitable and interoperable data governance is relevant to SDG 17. The commitment to enhance international governance of artificial intelligence is relevant to SDG 9, SDG 16, and SDG 17.

The Observatory's measurement framework is designed to capture progress against the Compact's commitments, which are in turn linked to the SDGs. The global implementation score of 69.2 out of 100 can be read as a proxy for the world's progress on the digital dimensions of the 2030 Agenda. The high-income to low-income implementation gap of 35.7 points can be read as a proxy for the digital dimension of the SDG implementation gap. The Observatory's commitment is to maintain this SDG linkage in subsequent editions, and to provide disaggregated analysis that supports the SDG follow-up and review process.

Chapter 2 — The GDC Governance Index 2025

2.1 Global Implementation Score

The global GDC Implementation Score for 2025 stands at 69.2 out of 100. This is the mean score across the 68 assessed countries. It should be interpreted as the mean score across the assessed countries, not as the score of the median global citizen.

Disaggregated by objective, Digital Safety and Security leads at 86.6. Data Governance follows at 72.3. Inclusive Digital Economy scores 66.1. Digital Divides scores 64.5. Artificial Intelligence governance records the lowest global score at 56.4.

2.2 Regional and Income-Group Analysis

Europe leads the regional implementation ranking with an average score of 83.5, followed by East Asia (77.2), Oceania (74.3), and North America (76.1). The Middle East and North Africa scores 71.6, Latin America and the Caribbean 67.8, Central Asia 67.2, Southeast Asia 63.7, South Asia 61.5, the CIS 66.4, and Sub-Saharan Africa 55.2.

Disaggregated by World Bank income group, high-income countries average 81.3 on implementation, upper-middle-income countries 67.5, lower-middle-income countries 60.1, and low-income countries 45.6. The high-income to low-income gap of 35.7 points is the single most consequential finding of this report.

2.3 Country Rankings and Dual Classification

The Observatory employs two separate classification systems. The Score Band distribution (based on Implementation Score alone) is: 15 Leaders, 27 Implementers, 21 Fragile Progress, 4 Stagnating, and 1 At Risk. The Three-Axis Profile distribution (based on Implementation x Capacity x Trajectory) is: 22 Leaders, 28 Implementers, 5 Fragile Progress, 1 Stagnating, and 12 At Risk.

The top five countries by Implementation Score are: Sweden (87.6), Singapore (87.5), Netherlands (87.2), United Kingdom (87.1), Norway (87.0).

2.4 The Equal-Weight Principle and Its Justification

The Observatory applies an equal-weight principle to the five GDC objectives: each objective carries 20 per cent of the Implementation Score. This principle is a substantive analytical choice and requires justification. The alternative approaches — weighting by the number of commitments per objective, weighting by the perceived importance of each objective, weighting by the implementation risk of each objective, or weighting by the financial resources required for implementation — each have merit, and each was considered. The Observatory chose equal weighting for three reasons. First, the Compact itself presents the five objectives as interlocking

and of equal normative standing; an unequal weighting would import an analytical judgement not present in the Compact's text. Second, equal weighting is the most transparent and the most reproducible; an unequal weighting would require a published rationale for each weight, and would invite contestation of each weight. Third, equal weighting produces the most stable country rankings under sensitivity analysis, as documented in Annex B; alternative weighting schemes produce larger swings in country rankings, particularly for countries near the boundaries between profiles.

The equal-weight principle does not imply that the five objectives are equally well-implemented. The global objective scores show substantial variation: Digital Safety and Security scores 86.6, Data Governance 72.3, Inclusive Digital Economy 66.1, Digital Divides 64.5, and Artificial Intelligence governance 56.4. The 30-point gap between the highest-scoring objective (Safety) and the lowest-scoring objective (AI) is one of the most consequential findings of this report. The equal-weight principle allows this variation to be visible; an unequal weighting that, for example, weighted AI at 40 per cent and the other four objectives at 15 per cent each would produce a different global headline figure but would obscure the implementation differential between objectives.

2.5 The Population-Weighted Alternative

The global Implementation Score of 69.2 is the unweighted mean of the 68 assessed countries. An alternative aggregation would weight each country by its population, producing a global score that reflects the experience of the median global citizen rather than the typical assessed country. The population-weighted alternative was tested as Specification E in the sensitivity analysis. The result is a different global headline figure, but the country-level classifications are not materially affected: the same countries appear in the Leader, Implementer, Fragile Progress, Stagnating, and At Risk profiles under both aggregations. The Observatory chose the unweighted aggregation for the headline figure because it treats each country as a unit of analysis equal to every other country, consistent with the UN's sovereign-equality principle. The population-weighted figure is reported in the sensitivity analysis for readers who prefer that aggregation.

The choice between unweighted and population-weighted aggregation is not merely technical; it is normative. The unweighted aggregation asks: how well is the average country implementing the Compact? The population-weighted aggregation asks: how well is the Compact being implemented for the average person? Both questions are legitimate, and the answers are different. The Observatory's view is that the country-level question is the primary question for an intergovernmental compact adopted by sovereign states, and that the population-level question is a secondary question best answered through disaggregated analysis. The 2026 edition will report both aggregations in the headline figures.

2.6 Country Ranking Analysis

The country rankings reveal several patterns worthy of detailed analysis. At the top of the ranking, Sweden (87.6) leads, followed closely by Singapore (87.5), the Netherlands (87.2), the United Kingdom (87.1), and Norway (87.0). The top five countries are separated by only 0.6 points, indicating a tightly clustered leadership cohort. The top ten includes Estonia (86.9), the United Arab Emirates (86.2), Australia (85.7), and New Zealand (85.1). The top fifteen extends through Germany (84.7), South Korea (84.4), Spain (84.4), France (84.3), and Japan (82.6). The composition of the top fifteen reflects the dominance of high-income countries, particularly in Europe, East Asia, and Oceania.

The middle of the ranking — countries ranked 16 through 50 — contains the most analytically interesting cases. Italy (79.7) and Saudi Arabia (79.6) are at the upper boundary of the Leader profile. China (79.5), Qatar (77.9), Poland (77.4), Israel (77.0), and Canada (76.8) form a substantial Leader cohort. Brazil (76.4), the United States (75.4), Greece (74.7), Chile (74.1), India (74.0), Malaysia (74.0), and Thailand (73.9) are classified as At Risk through the transitional-zone Rule 4 (Improving, Implementation 73.5 to 77, Capacity below 80), or in the case of the United States, because its trajectory is Deteriorating (Rule 1). This middle band of At Risk countries is the most consequential finding of the country ranking analysis: these are countries with substantial implementation that are nonetheless at risk of stalling or reversing.

The bottom of the ranking — countries ranked 51 through 68 — includes the Fragile Progress, Stagnating, and At Risk cohorts. Rwanda (62.0), Peru (62.0), Bangladesh (61.5), Jamaica (60.8), and Egypt (60.6) are classified as Implementer despite lower implementation scores, because their trajectories are Improving. Cote d'Ivoire (55.9), Tanzania (54.6), Pakistan (53.0), Nepal (52.9), and Fiji (52.1) are classified as Fragile Progress. Tunisia (54.4) is At

Risk on a Deteriorating trajectory. Senegal (43.1), Cambodia (41.5), Uganda (41.3), and Myanmar (34.0) are At Risk on Stagnating trajectories with implementation below 45. Ethiopia (45.2) is the sole Stagnating profile country in the assessed sample, classified under Rule 2 (Stagnating trajectory with Implementation at least 45). The bottom of the ranking is dominated by low-income and lower-middle-income countries in Sub-Saharan Africa, South Asia, and Southeast Asia.

The most striking outlier in the ranking is the United States (75.4), which ranks 24th overall but is classified as At Risk due to its Deteriorating trajectory and Forward Score of 37.6. The United States is the only high-income country with a Deteriorating trajectory in the assessed sample. The drivers of this deterioration — the volatility of federal AI policy, the absence of a comprehensive federal data-protection law, and the erosion of regulatory predictability — are documented in detail in Chapter 7. The US case illustrates the value of the Three-Axis Profile system: a single-score ranking would place the United States in the upper-middle of the distribution, but the three-axis assessment reveals the forward-looking risk that the single score conceals.

2.7 Top-Performing Countries: Detailed Profiles

The top-performing countries in the inaugural assessment warrant detailed profile analysis. Sweden (87.6), the highest-ranked country, combines comprehensive digital governance institutions, robust data-protection legislation, mature cybersecurity capacity (GCI Tier 1), and a forward-looking AI strategy. Sweden's Objectives scores — Divides: 90.7, Economy: 90.5, Safety: 95.2, Data: 86.7, AI: 74.7 — are uniformly high, with no objective scoring below 70. Singapore (87.5), the second-ranked country, combines world-class digital government, advanced digital public infrastructure, and a comprehensive AI governance framework. Singapore's position as a global digital hub is reflected in its high scores across all five objectives.

The Netherlands (87.2), the third-ranked country, combines robust data-protection legislation (implementing the GDPR), advanced e-government, and a forward-looking national AI strategy. The United Kingdom (87.1), the fourth-ranked country, combines comprehensive digital governance institutions, mature cybersecurity capacity, and a world-leading AI safety institute (the AI Safety Institute, established November 2023). Norway (87.0), the fifth-ranked country, combines comprehensive digital government, robust data-protection legislation, and high digital inclusion. The top five countries are separated by only 0.6 points, indicating a tightly clustered leadership cohort where small differences in indicator scores produce small differences in the overall ranking.

The next ten countries — Estonia (86.9), the United Arab Emirates (86.2), Australia (85.7), New Zealand (85.1), Germany (84.7), South Korea (84.4), Spain (84.4), France (84.3), Japan (82.6), and Portugal (80.7) — form a broader leadership cohort. These countries share several characteristics: comprehensive digital governance institutions, robust data-protection legislation, mature cybersecurity capacity, and forward-looking AI strategies. The variation within this cohort reflects differences in digital public infrastructure maturity (Estonia, Singapore, and the UAE are leaders), in cybersecurity capacity (South Korea and Israel are leaders), and in AI governance (the UK, Singapore, and Japan are leaders).

2.8 Bottom-Performing Countries: Structural Deficits

The bottom-performing countries in the inaugural assessment warrant detailed profile analysis, particularly to identify the structural deficits that constrain implementation. Myanmar (34.0), the lowest-ranked country, faces a combination of political instability, low internet penetration (26.0 per cent), and limited digital governance institutions. Uganda (41.3), the second-lowest-ranked country, faces similar structural constraints, including low internet penetration (27.0 per cent) and limited digital governance capacity. Cambodia (41.5), the third-lowest-ranked country, faces a combination of low cybersecurity capacity, limited digital public infrastructure, and restrictive cross-border data-flow regime.

Senegal (43.1), Ethiopia (45.2), and Cote d'Ivoire (55.9) form the next tier of low-performing countries. These countries share several structural deficits: low internet penetration, limited digital public infrastructure, low cybersecurity capacity, and limited data-protection legislation. The structural deficits are not amenable to short-term policy intervention; they require sustained, multi-year investment in digital infrastructure, digital skills, digital governance institutions, and digital economy development. The Observatory's recommendation is that the international community, through the proposed Global Fund for AI and other financing mechanisms, should prioritise the structural deficit countries for comprehensive capacity-building support.

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

The middle of the ranking — countries ranked 16 through 50 — is the most analytically interesting band. This band includes the Leader countries that are at the upper boundary of the Leader profile (Italy, Saudi Arabia), the upper-middle-income countries that have achieved Leader status (China, Poland), and the At Risk countries that have substantial implementation but face forward-looking risks (Brazil, the United States, Greece, Chile, India, Malaysia, Thailand). The middle band is where the most consequential policy interventions are needed: the Leader countries need to sustain their momentum, the upper-middle-income Leaders need to consolidate their gains, and the At Risk countries need to address their forward-looking risks. The Observatory's analysis of the middle band is the focus of Chapter 8 (the three-axis country assessment) and Chapter 9 (the Forward Readiness and Risk Monitor).

PART II

THE FIVE OBJECTIVES

Chapter 3 — Objective 1: Closing Digital Divides

3.1 Global Assessment

The AUN GDC Governance Index scores the global implementation of this objective at 64.5 out of 100 for 2025. According to the ITU's Facts and Figures 2025 report, published on 17 November 2025, approximately 6 billion people are now online (roughly 74 per cent of the world's population), and 2.2 billion remain offline. The ITU revised its 2024 estimate of the offline population downward from 2.6 billion to 2.3 billion, reflecting improved measurement and accelerated connectivity deployment.

3.2 Implementation Drivers and Barriers

Four implementation drivers are visible in the data. The first is the rapid expansion of mobile broadband networks, which now cover 95 per cent of the global population. The gap between network coverage and actual usage is the more consequential divide: an estimated 3.4 billion people live in areas covered by mobile broadband but do not use it, primarily because of affordability, skills, and relevance constraints. The second driver is the proliferation of digital public infrastructure, particularly in middle-income countries. The 50-in-5 initiative, launched at the GDC's adoption, commits countries to design and deliver inclusive, safe, and secure DPI by 2028. The third driver is the gradual closing of the digital gender divide, though progress is uneven and slow. The ITU estimates that 244 million more men than women use the internet globally. The fourth driver is the expansion of digital skills programmes, though the quality and reach of these programmes vary considerably.

Four implementation barriers are equally visible. The first is the affordability barrier, which remains the single most important obstacle to meaningful connectivity in the Global South. In the least developed countries, mobile broadband costs an average of 8 per cent of monthly GNI per capita. The Broadband Commission's target of 2 per cent or less is met in only 130 of 205 economies. The second barrier is the infrastructure barrier: connecting the remaining 2.2 billion offline population requires investment in resilient digital infrastructure. The third barrier is the skills and relevance barrier: even where infrastructure exists and is affordable, adoption requires digital literacy, content in local languages, and applications that address locally salient needs. The fourth barrier is the political barrier: in several jurisdictions, connectivity is treated as a strategic asset rather than a public good, and internet shutdowns, throttling, and selective access are used as instruments of political control.

3.3 Forward-Looking Risks

The Forward Risk Monitor identifies three emerging risks specific to the digital divides objective. The first is the risk of a connectivity plateau in which the marginal cost of connecting each additional person rises faster than the available financing. The second is the risk of a meaningful connectivity gap in which the headline metric of internet penetration improves while the underlying quality of connectivity stagnates. The third is the risk of a DPI backlash in which the rapid deployment of digital public infrastructure outpaces the development of safeguards.

Chapter 4 — Objective 2: Inclusive Digital Economy

4.1 Global Assessment

The AUN GDC Governance Index scores the global implementation of this objective at 66.1 out of 100 for 2025. The UNCTAD Technology and Innovation Report 2025 documents that the digital economy is concentrated geographically: the United States and China together account for approximately 75 per cent of global cloud computing capacity and 60 per cent of AI-related patents.

4.2 Implementation Drivers and Barriers

The implementation of the inclusive digital economy objective is driven by four interlocking trends. The first is the rapid expansion of digital financial inclusion, particularly through mobile money. The GSMA's State of the Industry Report on Mobile Money 2024 documents that registered mobile money accounts reached 1.7 billion globally in 2024, with daily transaction value exceeding $3.3 billion. The second driver is the expansion of e-government services, measured by the UN E-Government Development Index (EGDI). The 2024 EGDI survey shows that 71.5 per cent of UN member states are now in the very high or high EGDI bands. Denmark, Estonia, and Singapore lead the global ranking. The third driver is the gradual expansion of cross-border digital trade, facilitated by the WTO Joint Statement Initiative on e-commerce. The fourth driver is the growth of digital labour platforms, which the International Labour Organization estimates now mediate work for approximately 435 million people globally.

Four implementation barriers are visible. The first is the MSME digitalisation gap. Micro, small and medium-sized enterprises account for approximately 90 per cent of businesses and 50 per cent of employment worldwide, but their digital adoption rates lag significantly behind large firms. The OECD's Going Digital 2024 update reports that only 30 per cent of SMEs in OECD countries sell online. The second barrier is the digital trade fragmentation risk, driven by the proliferation of data-localisation requirements. The ITIF's 2024 data-localisation tracker identifies 144 measures in 65 countries. The third barrier is the digital skills mismatch. The World Economic Forum's Future of Jobs Report 2025 projects that, over the 2025-2030 period, approximately 170 million new jobs will be created globally while 92 million existing jobs will be displaced, resulting in a net increase of 78 million jobs and a structural job churn rate of 22 per cent. The fourth barrier is the platform power concentration risk.

Chapter 5 — Objective 3: Digital Safety and Security

5.1 Global Assessment

The AUN GDC Governance Index scores the global implementation of this objective at 86.6 out of 100 for 2025 — the highest of the five objectives. The ITU's Global Cybersecurity Index 2024 reports that 46 countries have achieved Tier 1 status, 29 are in Tier 2, 49 in Tier 3, 56 in Tier 4, and 14 in Tier 5. The Tier 1 cohort includes many — but not all — Western European countries, the United States, Canada, Australia, New Zealand, Japan, South Korea, Singapore, India, China, Brazil, and several African states.

5.2 Implementation Drivers and Barriers

Four implementation drivers are visible. The first is the institutionalisation of national cybersecurity strategies: 132 countries have a published national cybersecurity strategy, up from 92 in 2020. The second driver is the expansion of computer emergency response teams: 118 countries have an operational national CERT. The third driver is the gradual maturation of cybersecurity workforce development. The (ISC)2 Cybersecurity Workforce Study 2024 estimates the global cybersecurity workforce at 7.5 million people, though the workforce gap remains at approximately 4 million. The fourth driver is the expansion of regional cybersecurity cooperation frameworks, including the Budapest Convention on Cybercrime (75 parties) and the African Union Malabo Convention (entered into force in 2023).

Four implementation barriers are equally visible. The first is the asymmetry between the rapidly evolving threat landscape and the slower pace of institutional adaptation. The World Economic Forum's Global Cybersecurity Outlook 2025 reports that 73 per cent of organisations experienced a significant cyber incident in the past year. The IBM Cost of a Data Breach Report 2024 estimates the average cost of a data breach at $4.88 million. The second barrier is the protection of human rights online, particularly in the context of surveillance, encryption, and content moderation. The third barrier is the protection of children online. The fourth barrier is the information

integrity challenge. The WEF Global Risks Report 2025 ranks AI-generated misinformation as the top global risk over the next two years.

Chapter 6 — Objective 4: Data Governance

6.1 Global Assessment

The AUN GDC Governance Index scores the global implementation of this objective at 72.3 out of 100 for 2025. 137 countries now have a data-protection law on the statute books. The European Commission's adequacy decisions, which recognise a third country's data-protection regime as equivalent to the GDPR, have been extended to 17 jurisdictions: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom, Uruguay, the United States (under the Data Privacy Framework), and others. The UAE is not on this list.

6.2 Implementation Drivers and Barriers

Four implementation drivers are visible. The first is the global diffusion of GDPR-influenced data-protection legislation. Of the 137 countries with data-protection laws, approximately 85 have enacted or substantially revised their legislation since the GDPR entered into force in 2018. The second driver is the gradual emergence of data-for-development frameworks. The third driver is the expansion of open data initiatives. The fourth driver is the emergence of data trusts, data cooperatives, and other institutional innovations for data stewardship.

Four implementation barriers are equally visible. The first is the fragmentation of cross-border data-flow regimes. The Observatory's composite cross-border data-flow indicator classifies a significant share of assessed countries as restrictive. The second barrier is the enforcement gap in data-protection legislation. The third barrier is the slow establishment of the institutional machinery the Compact mandates, particularly the CSTD working group on data governance. The fourth barrier is the data-colonialism concern — the current data-governance architecture disproportionately benefits a small number of jurisdictions and firms.

Chapter 7 — Objective 5: Artificial Intelligence

This chapter receives deeper analytical treatment than the preceding four, reflecting the rapidity of institutional change in the AI governance domain, the concentration of regulatory developments in 2024-2025, the magnitude of implementation uncertainty, and the importance of AI governance to the Compact's future review architecture. The deeper treatment does not imply greater formal weight: AI carries 20 per cent of the implementation score, on equal footing with the other four objectives.

7.1 Global Assessment

The AUN GDC Governance Index scores the global implementation of this objective at 56.4 out of 100 for 2025 — the lowest of the five objectives. The Stanford HAI AI Index 2025 reports that total corporate AI investment in 2024 reached $252.3 billion, with the United States accounting for $109.1 billion in private investment and China $9.3 billion. Generative AI investment reached $33.9 billion in 2024.

7.2 Implementation Drivers and Barriers

Four implementation drivers are visible. The first is the rapid proliferation of national AI strategies. The OECD AI Policy Observatory reports that over 80 jurisdictions have published a national AI strategy as of late 2025, up from 44 in 2020. The African Union's Continental AI Strategy, endorsed by the Executive Council in July 2024, is the first regional AI strategy covering 55 member states. The second driver is the gradual maturation of regulatory frameworks. The EU AI Act, which entered into force on 1 August 2024, is the world's first comprehensive horizontal AI regulation. The third driver is the expansion of AI safety institutions. The United Kingdom established the world's first AI Safety Institute in November 2023. The AI Safety Institutes Network, launched at the Seoul AI Summit in May 2024, now includes 12 member institutions. The fourth driver is the elaboration of voluntary commitments by frontier AI developers.

Four implementation barriers are equally visible. The first is the AI capability divide. The Oxford Insights AI Readiness Index 2024 reports that the top 10 countries account for approximately 50 per cent of global AI readiness. The second barrier is the incomplete establishment of the international institutional architecture the Compact mandates. The General Assembly's adoption of resolution 79/325 on 26 August 2025 was a significant

milestone, but the 40 members of the Scientific Panel are expected to be appointed in early 2026, and the first convening of the Global Dialogue is scheduled for July 2026. The third barrier is the rapid evolution of AI capabilities, which outpaces the pace of regulatory and institutional adaptation. The fourth barrier is the geopolitical contestation of AI governance.

7.3 Forward-Looking Risks

The Forward Risk Monitor identifies four emerging risks. The first is the risk of a capability divide widening. The second is the risk of a regulatory fragmentation cascade. The third is the risk of an AI-enabled information crisis. The fourth is the risk of a workforce displacement shock, with the WEF Future of Jobs 2025 projecting 92 million jobs displaced and 170 million created over 2025-2030.

3.4 Detailed Drivers and Barriers Analysis

The four implementation drivers identified in Section 3.2 operate through distinct mechanisms and produce distinct patterns of progress. The first driver — the rapid expansion of mobile broadband networks — operates through infrastructure investment, primarily by mobile network operators responding to commercial incentives and regulatory frameworks that encourage or mandate network expansion. Mobile broadband coverage now reaches 95 per cent of the global population, but the gap between coverage and usage — the so-called usage gap — is the more consequential divide. An estimated 3.4 billion people live in areas covered by mobile broadband but do not use it, primarily because of affordability, skills, and relevance constraints. The coverage-to-usage conversion rate varies substantially by region: it is highest in Europe and North America, where coverage and usage are nearly coextensive, and lowest in Sub-Saharan Africa and South Asia, where the usage gap is largest.

The second driver — the proliferation of digital public infrastructure — operates through government-led investment in identity, payments, and data-exchange layers. The 50-in-5 initiative, launched at the GDC's adoption in September 2024, commits countries to design and deliver inclusive, safe, and secure DPI by 2028. As of late 2025, over 50 countries have joined the initiative. The DPI proliferation is most advanced in middle-income countries, particularly India (Aadhaar, UPI, DigiLocker), Brazil (Pix, gov.br), and Estonia (e-ID, X-Road), and is expanding rapidly in Africa (the Africa Digital Public Infrastructure initiative supported by the African Union, the African Development Bank, and the World Bank). The DPI driver is significant because it creates the foundational infrastructure on which other digital services — financial inclusion, e-government, digital health, digital education — can be built.

The third driver — the gradual closing of the digital gender divide — operates through a combination of policy attention, programme intervention, and market dynamics. The ITU estimates that 244 million more men than women use the internet globally, down from 277 million in 2020. The gender divide is widest in Sub-Saharan Africa and South Asia, where cultural, economic, and educational barriers disproportionately exclude women from digital participation. The EQUALS Partnership, the Generation Equality Forum's Technology and Innovation Action Coalition, and a range of national-level programmes have contributed to the gradual narrowing of the divide. The fourth driver — the expansion of digital skills programmes — operates through formal education systems, vocational training, and employer-led upskilling. The quality and reach of these programmes vary considerably, and the skills mismatch documented in the WEF Future of Jobs Report 2025 remains a significant barrier.

The four implementation barriers identified in Section 3.2 are equally consequential. The affordability barrier remains the single most important obstacle to meaningful connectivity in the Global South. In the least developed countries, mobile broadband costs an average of 8 per cent of monthly GNI per capita, four times the Broadband Commission's target of 2 per cent or less. The affordability barrier is compounded by device costs: a basic smartphone costs more than 5 per cent of annual income for the poorest 20 per cent of the population in many low-income countries. The infrastructure barrier is concentrated in remote, rural, and marginalised communities where the marginal cost of network extension exceeds the commercial return. Connecting the remaining 2.2 billion offline population requires investment in resilient digital infrastructure, including backhaul, last-mile connectivity, and alternative technologies such as satellite and high-altitude platforms.

The skills and relevance barrier operates even where infrastructure exists and is affordable. Adoption requires digital literacy, content in local languages, and applications that address locally salient needs. The digital skills gap is particularly acute for women, older adults, and rural populations. The relevance gap is particularly acute

for linguistic minorities: the proportion of online content in any given language is roughly proportional to the number of speakers of that language with internet access, which means that speakers of low-resource languages have access to a disproportionately small body of online content. The political barrier — the use of internet shutdowns, throttling, and selective access as instruments of political control — is the most consequential barrier in a subset of jurisdictions. The Shutdown Tracker, maintained by Access Now, documented 196 internet shutdowns in 2024, affecting over 1.5 billion people. The political barrier is not amenable to technical or financial intervention; it requires political and diplomatic engagement.

3.5 Forward-Looking Risks: Detailed Analysis

The three forward-looking risks identified in Section 3.3 warrant detailed analysis. The first is the risk of a connectivity plateau, in which the marginal cost of connecting each additional person rises faster than the available financing. The ITU's connectivity trajectory shows that the annual increase in the online population has slowed from approximately 300 million per year in the 2015-2020 period to approximately 200 million per year in the 2020-2025 period. If this trajectory continues, the world will reach approximately 92 per cent online by 2030 — short of the Compact's commitment to connect the remaining offline population. The connectivity plateau is driven by the increasing concentration of the offline population in remote, rural, low-income, and politically marginalised contexts where the cost of connection is highest and the commercial return is lowest.

The second risk is the meaningful connectivity gap, in which the headline metric of internet penetration improves while the underlying quality of connectivity stagnates. The Alliance for Affordable Internet's Meaningful Connectivity framework — which uses four thresholds (device, network, frequency of use, speed) — finds that only approximately one-third of the world's population currently enjoys meaningful connectivity. The headline metric of 74 per cent online (ITU F&F 2025) overstates the reality of digital inclusion if meaningful connectivity is the appropriate standard. The meaningful connectivity gap is particularly wide in low-income and lower-middle-income countries, where the gap between basic and meaningful connectivity can exceed 40 percentage points.

The third risk is the DPI backlash, in which the rapid deployment of digital public infrastructure outpaces the development of safeguards. Digital public infrastructure — identity, payments, data exchange — creates concentrated benefits (financial inclusion, service delivery efficiency, government transparency) but also concentrated risks (data breaches, surveillance, exclusion of marginalised groups). Without robust safeguards — legal, technical, institutional — the DPI backlash could slow or reverse the deployment of digital public infrastructure, with significant consequences for the Compact's connectivity, economy, and data governance objectives. The Observatory's recommendation, set out in Chapter 12, is that a global DPI safeguards framework should be developed through a multi-stakeholder process convened by end 2026.

3.6 The Connectivity Plateau Risk

The connectivity plateau risk is one of the most consequential forward-looking risks to the Compact's digital divides objective. The ITU's connectivity trajectory shows that the annual increase in the online population has slowed from approximately 300 million per year in the 2015-2020 period to approximately 200 million per year in the 2020-2025 period. If this trajectory continues, the world will reach approximately 92 per cent online by 2030 — short of the Compact's commitment to connect the remaining offline population. The connectivity plateau is driven by the increasing concentration of the offline population in remote, rural, low-income, and politically marginalised contexts where the cost of connection is highest and the commercial return is lowest.

The policy response to the connectivity plateau includes several elements. The first is the deployment of alternative connectivity technologies — satellite constellations (Starlink, OneWeb, Kuiper), high-altitude platform stations (HAPS), and community networks — that can reach remote and rural populations at lower cost than traditional terrestrial infrastructure. The second is the reform of regulatory frameworks to enable infrastructure sharing, spectrum sharing, and innovative licensing models that reduce the cost of network extension. The third is the mobilisation of blended finance — combining public, private, and philanthropic capital — to de-risk infrastructure investment in commercially marginal markets. The fourth is the prioritisation of last-mile connectivity in national digital strategies, supported by universal service funds and other financing mechanisms. The Observatory's recommendation is that the connectivity plateau risk should be a priority agenda item for the WSIS+20 outcome document and the joint WSIS-GDC implementation roadmap.

3.7 The Meaningful Connectivity Framework

The meaningful connectivity framework, developed by the Alliance for Affordable Internet, uses four thresholds to define meaningful connectivity: a device (a smartphone or larger device), a network (a 4G or higher connection), frequency of use (daily), and speed (a sufficient speed for productive use). The framework finds that only approximately one-third of the world's population currently enjoys meaningful connectivity, compared to the headline figure of 74 per cent online (ITU F&F 2025). The meaningful connectivity gap is particularly wide in low-income and lower-middle-income countries, where the gap between basic and meaningful connectivity can exceed 40 percentage points. The Observatory's view is that the meaningful connectivity framework should be adopted as the standard for measuring progress against the Compact's connectivity commitments, and that the 2026 edition of this report will include meaningful connectivity indicators alongside the basic connectivity indicators.

The meaningful connectivity framework has implications for the Compact's commitment to close all digital divides. If the standard is basic internet access (any device, any network, any frequency, any speed), the world is on track to reach approximately 92 per cent by 2030. If the standard is meaningful connectivity (smartphone, 4G+, daily, sufficient speed), the world is on track to reach approximately 50-60 per cent by 2030 — far short of the Compact's commitment. The choice of standard is not merely technical; it is normative. The Observatory's view is that the Compact's commitment to close all digital divides should be interpreted as a commitment to meaningful connectivity, not merely basic access, and that the international community should adopt the meaningful connectivity framework as the standard for measuring progress.

4.3 Detailed Drivers and Barriers Analysis

The four implementation drivers identified in Section 4.2 operate through distinct mechanisms. The digital financial inclusion driver operates through the rapid expansion of mobile money, particularly in Sub-Saharan Africa (M-Pesa in Kenya, MTN Mobile Money in West Africa, Airtel Money in multiple markets) and South Asia (bKash in Bangladesh, Easypaisa in Pakistan). The GSMA's State of the Industry Report on Mobile Money 2024 documents that registered mobile money accounts reached 1.7 billion globally in 2024, with daily transaction value exceeding $3.3 billion. Mobile money has driven financial inclusion in markets where traditional banking infrastructure was sparse, but the gender gap in mobile money adoption remains significant: women are 33 per cent less likely than men to have a mobile money account in low- and middle-income countries.

The e-government driver operates through the maturation of national digital government platforms, measured by the UN E-Government Development Index (EGDI). The 2024 EGDI survey shows that 71.5 per cent of UN member states are now in the very high or high EGDI bands, up from 57 per cent in 2020. Denmark, Estonia, and Singapore lead the global ranking. The e-government driver is significant because it creates the digital service delivery infrastructure on which broader digital economy activity depends: citizens who interact with government online are more likely to transact online commercially, and businesses that interact with government online are more likely to participate in the digital economy. The cross-border digital trade driver operates through the WTO Joint Statement Initiative on e-commerce, which is negotiating rules on digital trade facilitation, data flows, and consumer protection. The fourth driver — the growth of digital labour platforms — operates through the proliferation of online work platforms (Upwork, Freelancer, Toptal) and location-based gig platforms (Uber, Glovo, Rappi). The International Labour Organization estimates that digital labour platforms now mediate work for approximately 435 million people globally.

The four implementation barriers are equally consequential. The MSME digitalisation gap is the first barrier. Micro, small and medium-sized enterprises account for approximately 90 per cent of businesses and 50 per cent of employment worldwide, but their digital adoption rates lag significantly behind large firms. The OECD's Going Digital 2024 update reports that only 30 per cent of SMEs in OECD countries sell online; the rate is substantially lower in non-OECD countries. The MSME gap is driven by a combination of factors: limited access to finance for digital investment, limited digital skills among MSME owners and employees, limited awareness of the commercial case for digital adoption, and limited availability of locally relevant digital tools and platforms. The digital trade fragmentation risk is the second barrier, driven by the proliferation of data-localisation requirements. The ITIF's 2024 data-localisation tracker identifies 144 measures in 65 countries, up from 49 measures in 35 countries in 2017. The fragmentation risk is significant because it raises the cost of cross-border digital trade, discriminates against smaller firms that cannot afford compliance costs, and creates barriers to entry for new digital services.

The digital skills mismatch is the third barrier. The World Economic Forum's Future of Jobs Report 2025 projects that, over the 2025-2030 period, approximately 170 million new jobs will be created globally while 92 million existing jobs will be displaced, resulting in a net increase of 78 million jobs and a structural job churn rate of 22 per cent. The skills demanded by the new jobs are not the same as the skills held by the workers displaced from the old jobs. The mismatch is most acute in middle-income countries, where the education and training systems are less responsive to labour market signals. The platform power concentration risk is the fourth barrier. The OECD's measurements of market concentration in digital platforms show that the top five firms account for over 70 per cent of global cloud computing revenue, over 80 per cent of search advertising revenue, and over 90 per cent of mobile operating system installations. The concentration is significant because it creates barriers to entry, raises concerns about rent extraction, and concentrates decision-making power over the digital economy in a small number of jurisdictions and firms.

4.4 MSME Digitalisation Gap Analysis

The MSME digitalisation gap warrants detailed analysis because MSMEs are the backbone of the global economy and their digital adoption is a critical determinant of the Compact's inclusive digital economy objective. The gap is multi-dimensional: it includes the basic digital adoption gap (use of email, websites, social media), the transactional digital adoption gap (e-commerce, digital payments, online booking), the operational digital adoption gap (cloud computing, enterprise resource planning, customer relationship management), and the strategic digital adoption gap (data analytics, artificial intelligence, digital business model innovation). Each dimension of the gap has different drivers and requires different policy responses.

The basic digital adoption gap is narrowing, driven by the decreasing cost of smartphones and the increasing reach of mobile broadband. The transactional digital adoption gap is wider and is driven by the cost and complexity of digital payment systems, the regulatory requirements for e-commerce (consumer protection, taxation, cross-border trade), and the competition from large e-commerce platforms. The operational digital adoption gap is wider still and is driven by the cost of cloud and software subscriptions, the skills required to deploy and maintain these tools, and the integration challenges with legacy systems. The strategic digital adoption gap is widest of all and is driven by the cost and complexity of AI and data analytics capabilities, the talent required to deploy these capabilities, and the strategic uncertainty about return on investment. The policy response to each dimension of the gap should be calibrated to the specific drivers: basic adoption requires connectivity and affordability; transactional adoption requires payment infrastructure and regulatory simplification; operational adoption requires skills development and finance; strategic adoption requires research and development support and access to AI infrastructure.

4.5 Digital Trade Fragmentation

The digital trade fragmentation risk is one of the most consequential barriers to the inclusive digital economy objective. The proliferation of data-localisation requirements — rules that require data to be stored or processed within a specific jurisdiction — has accelerated since 2018, driven by a combination of privacy concerns, security concerns, industrial policy considerations, and sovereignty considerations. The ITIF's 2024 data-localisation tracker identifies 144 measures in 65 countries. The fragmentation has several consequences. First, it raises the cost of cross-border digital trade: firms operating across multiple jurisdictions must maintain separate data infrastructure in each, raising capital and operating costs. Second, it discriminates against smaller firms that cannot afford compliance costs, creating barriers to entry and entrenching incumbent platforms. Third, it creates interoperability challenges: data that is stored in one jurisdiction cannot easily be transferred to another for processing, analysis, or service delivery. Fourth, it creates regulatory uncertainty: firms operating across multiple jurisdictions face a patchwork of conflicting or inconsistent rules.

The Compact's commitment to advance responsible, equitable and interoperable data governance is directly relevant to the fragmentation risk. The CSTD working group on data governance, mandated by the Compact, is expected to address cross-border data-flow interoperability as a priority. The Observatory's recommendation, set out in Chapter 12, is that the CSTD working group should be accelerated and should prioritise the development of interoperability principles for cross-border data flows. The interoperability approach is preferable to the harmonisation approach (which would require all jurisdictions to adopt identical rules, an unrealistic prospect) and to the bilateral approach (which would require a patchwork of bilateral agreements, an inefficient prospect).

4.6 Workforce Displacement and the Skills Mismatch

The WEF Future of Jobs Report 2025 projects that, over the 2025-2030 period, approximately 170 million new jobs will be created globally while 92 million existing jobs will be displaced, resulting in a net increase of 78 million jobs and a structural job churn rate of 22 per cent. The displacement is concentrated in clerical and administrative roles, manual production roles, and traditional retail roles. The creation is concentrated in technology roles (AI and machine learning specialists, data analysts, cybersecurity specialists), sustainability roles (renewable energy engineers, sustainability specialists), and care roles (healthcare professionals, social workers). The mismatch between displaced and created jobs is the central challenge: workers displaced from clerical roles cannot immediately transition to AI specialist roles without substantial retraining.

The workforce displacement challenge is particularly acute in middle-income countries, where the education and training systems are less responsive to labour market signals and where the social safety net is less robust. The challenge is also acute in lower-middle-income countries that have built export-oriented services sectors around business process outsourcing: these sectors are highly susceptible to AI-driven displacement. The policy response includes investment in reskilling and upskilling programmes, reform of education systems to emphasise digital and cognitive skills, and the development of social safety nets that can support workers through transition periods. The Compact's commitment to expand inclusion in and benefits from the digital economy must include explicit attention to the displacement challenge; net job creation does not automatically translate into inclusive outcomes if the displaced workers are not the same as the newly employed.

4.7 The Digital Public Infrastructure Driver

The digital public infrastructure driver is one of the most consequential implementation drivers for the inclusive digital economy objective. Digital public infrastructure — identity, payments, data exchange — creates the foundational infrastructure on which broader digital economy activity depends. The 50-in-5 initiative, launched at the GDC's adoption in September 2024, commits countries to design and deliver inclusive, safe, and secure DPI by 2028. As of late 2025, over 50 countries have joined the initiative. The DPI driver is most advanced in middle-income countries, particularly India (Aadhaar, UPI, DigiLocker), Brazil (Pix, gov.br), and Estonia (e-ID, X-Road). The DPI driver is significant because it creates concentrated benefits (financial inclusion, service delivery efficiency, government transparency) but also concentrated risks (data breaches, surveillance, exclusion of marginalised groups).

The Observatory's data show that countries with mature DPI tend to score higher on the Inclusive Digital Economy objective. India's Objective 2 score is 71.9, Brazil's is 73.6, and Estonia's is 92.6, all above the global average of 66.1. The correlation between DPI maturity and Objective 2 score is positive and significant, suggesting that DPI is a critical enabler of inclusive digital economy outcomes. The policy implication is that investment in DPI should be a priority for countries seeking to improve their Objective 2 performance, and that the DPI safeguards framework (Recommendation 3 in Chapter 12) should be developed as a complement to DPI investment, ensuring that the risks of DPI deployment are adequately managed.

4.8 The Cross-Border Digital Trade Driver

The cross-border digital trade driver is one of the most consequential implementation drivers for the inclusive digital economy objective, but it is also one of the most contested. The WTO Joint Statement Initiative on e-commerce, launched in 2017, is negotiating rules on digital trade facilitation, data flows, and consumer protection. The negotiations involve approximately 90 WTO members, accounting for over 90 per cent of global digital trade. The negotiations have made progress on several issues (electronic signatures, electronic transactions, paperless trading) but have stalled on the more contentious issues (data flows, data localisation, source code disclosure). The stalling reflects deep divisions between members that favour liberalisation (the United States, the European Union, Japan, Australia, Singapore, Canada) and members that favour restriction (China, India, Indonesia, Vietnam, Russia).

The cross-border digital trade driver is also affected by the proliferation of regional trade agreements with digital trade chapters. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Digital Economy Partnership Agreement (DEPA), the United States-Mexico-Canada Agreement (USMCA), and the Regional Comprehensive Economic Partnership (RCEP) all include digital trade provisions. The proliferation of regional agreements creates a patchwork of overlapping and sometimes inconsistent rules, raising compliance complexity for firms operating across multiple jurisdictions. The Observatory's recommendation is that the WTO

Joint Statement Initiative should be revitalised, with priority on the less contentious issues, and that the regional agreements should be harmonised through mutual recognition and interoperability principles.

5.3 Detailed Drivers and Barriers Analysis

The four implementation drivers identified in Section 5.2 operate through distinct mechanisms. The institutionalisation of national cybersecurity strategies is the first driver: 132 countries have a published national cybersecurity strategy, up from 92 in 2020. The strategies vary substantially in their scope, specificity, and implementation status, but the existence of a strategy is a necessary first step toward systematic cybersecurity capacity-building. The expansion of computer emergency response teams is the second driver: 118 countries have an operational national CERT. The CERTs vary in their capability and mandate, but they form the backbone of national cyber-incident response. The maturation of cybersecurity workforce development is the third driver: the (ISC)2 Cybersecurity Workforce Study 2024 estimates the global cybersecurity workforce at 7.5 million people, though the workforce gap remains at approximately 4 million. The expansion of regional cybersecurity cooperation frameworks is the fourth driver: the Budapest Convention on Cybercrime (75 parties), the African Union Malabo Convention (entered into force in 2023), and the ASEAN Cybersecurity Coordination Committee provide frameworks for cross-border cooperation on cybercrime investigation, incident response, and capacity-building.

The four implementation barriers are equally consequential. The asymmetry between the threat landscape and the institutional adaptation is the first barrier. The World Economic Forum's Global Cybersecurity Outlook 2025 reports that 73 per cent of organisations experienced a significant cyber incident in the past year. The IBM Cost of a Data Breach Report 2024 estimates the average cost of a data breach at $4.88 million. The threat landscape is evolving rapidly, driven by the professionalisation of cybercrime (the growth of ransomware-as-a-service and initial-access-broker markets), the geopolitical use of cyber operations (state-sponsored intrusion and disruption campaigns), and the weaponisation of AI for both attack and defence. The institutional adaptation is slower, constrained by the scarcity of skilled cybersecurity professionals, the cost of security tooling, and the complexity of securing heterogeneous digital environments. The protection of human rights online is the second barrier, particularly in the context of surveillance, encryption, and content moderation. The protection of children online is the third barrier. The information integrity challenge is the fourth barrier.

5.4 The Cyber-Resilience Gap

The cyber-resilience gap — the difference between the cyber-resilience of well-resourced organisations and that of less-resourced organisations — is one of the most consequential barriers to the Compact's digital safety and security objective. The gap is multi-dimensional. The financial dimension: large organisations can afford comprehensive security tooling, dedicated security teams, and cyber insurance; small organisations cannot. The talent dimension: large organisations can attract and retain skilled cybersecurity professionals; small organisations cannot. The technical dimension: large organisations can implement defence-in-depth architectures with multiple layers of detection, prevention, and response; small organisations typically rely on basic antivirus and firewall solutions. The institutional dimension: large organisations have formal incident response plans, tested through exercises; small organisations typically have informal or ad hoc arrangements.

The cyber-resilience gap is particularly acute in three contexts. The first is MSMEs, which are the backbone of most economies but have the least cyber-resilience. The second is critical infrastructure operators in lower-income countries, where the convergence of operational technology and information technology has created new attack surfaces without corresponding investment in security. The third is government agencies in lower-income countries, which often lack the resources to defend against sophisticated cyber operations. The policy response to the cyber-resilience gap includes subsidised security tooling for MSMEs, capacity-building programmes for critical infrastructure operators, and international cooperation on incident response. The Observatory's recommendation, set out in Chapter 12, is that the cyber-resilience gap should be addressed through targeted capacity-building programmes supported by the proposed Global Fund for AI and digital cooperation.

5.5 The AI-Enabled Information Crisis

The AI-enabled information crisis is one of the most consequential emerging risks to the Compact's digital safety and security objective. The WEF Global Risks Report 2025 ranks AI-generated misinformation as the top global risk over the next two years. The risk is driven by the rapid improvement of generative AI capabilities — text

generation, image generation, video generation, voice cloning — and the corresponding reduction in the cost of producing high-quality synthetic content. The risk manifests in several ways: the proliferation of synthetic content in political processes (election interference, voter manipulation, disinformation campaigns), the erosion of trust in media and information sources, the weaponisation of synthetic content for fraud and extortion, and the manipulation of financial markets through false information.

The policy response to the AI-enabled information crisis includes several elements. The first is content provenance: cryptographic and watermarking techniques that allow the origin and modification history of digital content to be verified. The Coalition for Content Provenance and Authenticity (C2PA) has developed a technical standard that is being adopted by major content platforms. The second is platform accountability: regulatory frameworks that require platforms to take reasonable steps to detect, label, and remove harmful synthetic content. The EU's Digital Services Act and AI Act include provisions relevant to this. The third is media literacy: educational programmes that help citizens identify synthetic content and verify the authenticity of information sources. The fourth is regulatory clarity on the permitted uses of generative AI, particularly in political and commercial contexts. The Observatory's recommendation is that the Global Dialogue on AI Governance, scheduled for July 2026, should prioritise the AI-enabled information crisis as one of its first substantive agenda items.

5.6 Child Online Protection

Child online protection is one of the most consequential dimensions of the Compact's digital safety and security objective, and one of the most under-addressed in the current implementation architecture. The WeProtect Global Alliance reports that online child sexual exploitation and abuse (CSEA) is increasing in volume, sophistication, and geographic reach, driven by the proliferation of digital platforms, the anonymisation of online interactions, and the cross-border nature of the threat. The threat is compounded by the rapid improvement of generative AI capabilities, which can be used to produce synthetic CSEA content, to groom children online, and to evade detection. The policy response to online CSEA includes several elements: legal frameworks (criminalising online CSEA and establishing extraterritorial jurisdiction), institutional frameworks (dedicated law enforcement units, hotlines, and reporting mechanisms), technical frameworks (detection, hashing, and removal technologies), and educational frameworks (digital literacy, online safety education, and parental awareness).

The Observatory's data show that child online protection is one of the weakest dimensions of the digital safety and security objective. The proxy indicator for child online safety, which combines GCI tier and cybercrime legislation status, shows substantial variation across the assessed countries. The variation reflects differences in legal frameworks (some countries have comprehensive child online protection legislation; others do not), in institutional capacity (some countries have dedicated law enforcement units; others do not), and in technical capacity (some countries have access to detection and removal technologies; others do not). The Observatory's recommendation is that child online protection should be a priority agenda item for the Global Dialogue on AI Governance, scheduled for July 2026, and that the proposed Global Fund for AI should include dedicated resources for child online protection capacity-building in the Global South.

5.7 The Surveillance and Encryption Challenge

The surveillance and encryption challenge is one of the most contested dimensions of the Compact's digital safety and security objective. The challenge arises from the tension between two legitimate concerns: the need for law enforcement and intelligence agencies to access communications for legitimate investigations, and the need for citizens and firms to protect their communications from unauthorised access, including access by state actors. The tension has been exacerbated by the proliferation of end-to-end encryption, which protects communications from access by anyone other than the sender and recipient, including the platform provider. The encryption debate has produced several policy responses: the EU's proposal for chat control (which would require platforms to scan encrypted communications for CSEA content), the United States' EARN IT Act (which would condition platform liability protection on compliance with best practices for child online safety), and the UK's Online Safety Act (which requires platforms to deploy accredited technology to identify CSEA content in encrypted communications).

The encryption debate is significant because it touches on fundamental questions about the balance between security and privacy, between state power and individual rights, and between the rule of law and technological autonomy. The Compact's commitment to foster an inclusive, open, safe and secure digital space should be interpreted to include explicit attention to the encryption debate, and to the broader question of surveillance reform.

The Observatory's recommendation is that the Global Dialogue on AI Governance should include encryption and surveillance as a substantive agenda item, and that the international community should develop principles for the governance of encryption that balance the legitimate concerns of law enforcement, intelligence, privacy, and security.

6.3 Detailed Drivers and Barriers Analysis

The four implementation drivers identified in Section 6.2 operate through distinct mechanisms. The global diffusion of GDPR-influenced data-protection legislation is the first driver. Of the 137 countries with data-protection laws, approximately 85 have enacted or substantially revised their legislation since the GDPR entered into force in 2018. The diffusion is driven by a combination of factors: the regulatory Brussels effect (firms operating globally have adopted GDPR-compliant practices as a default), the demonstration effect (jurisdictions have observed the GDPR's impact and chosen to emulate it), and the trade effect (the EU's adequacy decision framework creates an incentive for third countries to adopt GDPR-equivalent regimes). The diffusion has produced a degree of convergence in data-protection standards, but the convergence is incomplete: substantial variation remains in scope, enforcement, and institutional capacity.

The gradual emergence of data-for-development frameworks is the second driver. The data-for-development agenda seeks to mobilise data — public, private, and civil society — for sustainable development outcomes. The Global Partnership for Sustainable Development Data, the UN World Data Forum, and a range of national-level open data initiatives have contributed to the emergence of this agenda. The driver is significant because it creates a positive case for data governance — data as an asset for development — that complements the defensive case (data as a risk to be managed). The expansion of open data initiatives is the third driver. The Open Data Barometer, the OECD OURdata Index, and a range of national-level open data portals have documented the gradual expansion of open data publication by governments. The driver is significant because open data creates transparency, accountability, and innovation opportunities. The emergence of data trusts, data cooperatives, and other institutional innovations for data stewardship is the fourth driver, and is the least mature of the four. These innovations seek to create institutional mechanisms for collective data governance that go beyond the individual-rights framework of traditional data-protection law.

The four implementation barriers are equally consequential. The fragmentation of cross-border data-flow regimes is the first barrier. The Observatory's composite cross-border data-flow indicator classifies a significant share of assessed countries as restrictive. The fragmentation is driven by a combination of legitimate concerns (privacy, security, law enforcement access) and protectionist considerations (industrial policy, support for domestic cloud providers). The enforcement gap in data-protection legislation is the second barrier. The 137 countries with data-protection laws on the statute books vary enormously in the enforcement capacity of their data-protection authorities. Many authorities are under-resourced, under-staffed, or politically constrained. The gap between law on the books and law in practice is one of the most significant barriers to the data governance objective. The slow establishment of the institutional machinery the Compact mandates, particularly the CSTD working group on data governance, is the third barrier. The data-colonialism concern is the fourth barrier.

6.4 Cross-Border Data Flow Fragmentation

The cross-border data-flow fragmentation is one of the most consequential barriers to the Compact's data governance objective. The fragmentation is driven by the proliferation of data-localisation requirements — rules that require data to be stored or processed within a specific jurisdiction. The fragmentation is also driven by the proliferation of distinct regulatory regimes for cross-border data transfer: the EU's adequacy decision framework (recognising third countries as providing equivalent protection to the GDPR), the EU's Standard Contractual Clauses (providing a contractual mechanism for transfer to non-adequate countries), the APEC Cross-Border Privacy Rules (providing a regional certification mechanism), and a range of national-level transfer mechanisms. The proliferation of regimes creates compliance complexity for firms operating across multiple jurisdictions, raises the cost of cross-border data flows, and creates interoperability challenges.

The Observatory's composite cross-border data-flow indicator classifies each assessed country as open (few or no restrictions), conditional (restrictions conditional on specific safeguards), or restrictive (significant restrictions on cross-border transfer). The classification is based on a composite of the EU adequacy decision status, the WTO Joint Statement Initiative position, and the ITIF data-localisation tracker. The classification is necessarily simplified: the actual regulatory landscape is more nuanced than a three-category classification can capture.

The classification is, however, a useful summary of the broad regulatory orientation of each jurisdiction. The Observatory's recommendation is that the CSTD working group on data governance, mandated by the Compact, should prioritise the development of interoperability principles for cross-border data flows. The interoperability approach does not require harmonisation of regulatory regimes; it requires mutual recognition and the development of bridging mechanisms that allow data to flow across regimes without violating the substantive protections of any regime.

6.5 The Enforcement Deficit

The enforcement deficit — the gap between the data-protection law on the books and the data-protection law in practice — is one of the most significant barriers to the Compact's data governance objective. The deficit manifests in several ways. The resource deficit: many data-protection authorities are under-funded and under-staffed relative to the scope of their mandate. The skills deficit: data-protection enforcement requires technical, legal, and investigative skills that are in short supply globally. The political deficit: data-protection authorities are sometimes politically constrained in their enforcement actions, particularly when the targets are powerful domestic firms or government agencies. The procedural deficit: data-protection enforcement often requires complex investigations that take years to complete, and the remedies available to authorities are sometimes disproportionate to the harms being addressed.

The enforcement deficit has several consequences. It undermines the deterrent effect of data-protection law: firms that calculate that enforcement is unlikely may choose to comply minimally rather than substantively. It creates a competitive disadvantage for compliant firms: firms that invest in robust data-protection compliance bear costs that non-compliant firms do not. It erodes public trust in data-protection frameworks: citizens who observe that data-protection law is not enforced may conclude that the law is not worth taking seriously. The policy response to the enforcement deficit includes increased resourcing for data-protection authorities, capacity-building programmes for enforcement staff, and the development of regional enforcement cooperation frameworks (the Global Privacy Assembly, the European Data Protection Board, the Asia Pacific Privacy Authorities forum).

6.6 The Data Colonialism Concern

The data-colonialism concern — the observation that the current data-governance architecture disproportionately benefits a small number of jurisdictions and firms, often at the expense of the Global South — is one of the most consequential critiques of the existing data-governance framework. The concern manifests in several ways. The extractive dynamic: data generated by users in the Global South is often processed, monetised, and stored in the Global North, with limited benefit accruing to the countries and communities where the data originated. The platform dependency: digital platforms based in the Global North often dominate the digital economies of the Global South, with limited local value capture. The talent drain: skilled data professionals from the Global South are often recruited by firms in the Global North, with limited retention in the countries of origin. The infrastructure dependency: cloud computing, AI, and other data-intensive infrastructure is often concentrated in the Global North, with limited local capacity in the Global South.

The data-colonialism concern is not merely a critique of the existing framework; it is also a critique of the existing framework's response. The GDPR and similar data-protection frameworks focus on individual rights (consent, access, rectification, erasure) but do not address the structural dynamics of data extraction, platform dependency, talent drain, and infrastructure dependency. The Compact's commitment to advance responsible, equitable and interoperable data governance should be interpreted to include explicit attention to the structural dimensions of data justice. The Observatory's recommendation is that the CSTD working group on data governance should include explicit consideration of the structural dimensions of data justice, including data sovereignty, benefit-sharing, and capacity-building for data-intensive industries in the Global South.

6.7 The GDPR Diffusion Dynamic

The GDPR diffusion dynamic is one of the most consequential implementation drivers for the Compact's data governance objective. Of the 137 countries with data-protection laws, approximately 85 have enacted or substantially revised their legislation since the GDPR entered into force in 2018. The diffusion is driven by a combination of factors: the regulatory Brussels effect (firms operating globally have adopted GDPR-compliant practices as a default), the demonstration effect (jurisdictions have observed the GDPR's impact and chosen to emulate it), and the trade effect (the EU's adequacy decision framework creates an incentive for third countries to adopt GDPR-

equivalent regimes). The diffusion has produced a degree of convergence in data-protection standards, but the convergence is incomplete: substantial variation remains in scope, enforcement, and institutional capacity.

The GDPR diffusion has produced several distinct models of data-protection legislation. The full-GDPR model, adopted by countries seeking EU adequacy (Japan, South Korea, the United Kingdom), closely follows the GDPR's structure, scope, and enforcement provisions. The adapted-GDPR model, adopted by countries that have emulated the GDPR but adapted it to local contexts (Brazil's LGPD, India's DPDP Act, Canada's proposed CPPA), follows the GDPR's broad structure but differs in specific provisions. The distinct model, adopted by countries that have developed their own data-protection frameworks (China's PIPL, the United States' sectoral approach), differs substantially from the GDPR in structure, scope, and enforcement. The Observatory's view is that the GDPR diffusion is a positive development for the Compact's data governance objective, but that the convergence should not be interpreted as harmonisation: the substantive standards, the enforcement practices, and the institutional capacities vary substantially across the diffused regimes.

6.8 The Open Data Agenda

The open data agenda is one of the most consequential implementation drivers for the Compact's data governance objective. Open data — data that is freely available, machine-readable, and reusable — creates transparency, accountability, and innovation opportunities. The Open Data Barometer, the OECD OURdata Index, and a range of national-level open data portals have documented the gradual expansion of open data publication by governments. The expansion is driven by a combination of factors: the transparency effect (open data enables citizens, journalists, and civil society to scrutinise government activity), the innovation effect (open data enables entrepreneurs and researchers to develop new products, services, and insights), and the efficiency effect (open data enables government agencies to share data internally and reduce duplication).

The open data agenda faces several challenges. The first is the quality challenge: much open data is incomplete, outdated, or inconsistent, limiting its usefulness for analysis and application. The second is the privacy challenge: some open data, particularly micro-level data, raises privacy concerns that require careful de-identification and aggregation. The third is the sustainability challenge: open data publication requires sustained investment in data infrastructure, data governance, and data literacy, and many open data initiatives have struggled to sustain this investment beyond the initial publication phase. The Observatory's recommendation is that the open data agenda should be integrated into the Compact's data governance implementation, with priority on high-value datasets (geospatial, statistical, budgetary, procurement) and on the development of data quality and privacy standards.

7.3 Detailed Drivers and Barriers Analysis

The four implementation drivers identified in Section 7.2 operate through distinct mechanisms. The rapid proliferation of national AI strategies is the first driver. The OECD AI Policy Observatory reports that over 80 jurisdictions have published a national AI strategy as of late 2025, up from 44 in 2020. The strategies vary substantially in their ambition, specificity, and implementation status. The African Union's Continental AI Strategy, endorsed by the Executive Council in July 2024, is the first regional AI strategy covering 55 member states and represents a significant milestone in the diffusion of AI governance norms to the African continent. The gradual maturation of regulatory frameworks is the second driver. The EU AI Act, which entered into force on 1 August 2024, is the world's first comprehensive horizontal AI regulation and establishes a risk-based framework that prohibits certain AI practices (social scoring, real-time biometric identification in public spaces), imposes stringent requirements on high-risk AI systems (employment, education, essential services, law enforcement), and imposes transparency obligations on limited-risk AI systems (chatbots, deepfakes).

The expansion of AI safety institutions is the third driver. The United Kingdom established the world's first AI Safety Institute in November 2023, following the Bletchley Park AI Safety Summit. The AI Safety Institutes Network, launched at the Seoul AI Summit in May 2024, now includes 12 member institutions: the United Kingdom, the United States, Japan, Singapore, Canada, France, Germany, Italy, the Republic of Korea, Australia, Ireland, and the European Union. The Institutes' mandate includes pre-deployment evaluation of frontier AI models, foundational AI safety research, and international cooperation on AI safety standards. The elaboration of voluntary commitments by frontier AI developers is the fourth driver. The White House voluntary commitments (July 2023, signed by seven leading AI developers), the Frontier AI Forum commitments (September 2024), and the Seoul AI Summit commitments (May 2024) have established a set of voluntary practices — including internal and

external red-teaming, information sharing, and safety incident reporting — that are increasingly being codified into binding regulation.

The four implementation barriers are equally consequential. The AI capability divide is the first barrier. The Oxford Insights AI Readiness Index 2024 reports that the top 10 countries account for approximately 50 per cent of global AI readiness, and the bottom 60 countries account for less than 10 per cent. The divide is multi-dimensional: it includes compute capacity (the concentration of advanced AI accelerators in a small number of jurisdictions), talent (the concentration of AI researchers and engineers in a small number of jurisdictions and firms), data (the concentration of large, high-quality training datasets in a small number of firms), and infrastructure (the concentration of cloud computing and AI infrastructure in a small number of jurisdictions and firms). The incomplete establishment of the international institutional architecture the Compact mandates is the second barrier. The General Assembly's adoption of resolution 79/325 on 26 August 2025 was a significant milestone, but the 40 members of the Scientific Panel are expected to be appointed in early 2026, and the first convening of the Global Dialogue is scheduled for July 2026.

The rapid evolution of AI capabilities is the third barrier. The pace of capability improvement in generative AI — measured by performance on standard benchmarks, by the breadth of tasks at which AI systems exceed human performance, and by the economic value created by AI applications — outpaces the pace of regulatory and institutional adaptation. The lag is significant because it creates a window during which AI capabilities are deployed without corresponding safeguards. The geopolitical contestation of AI governance is the fourth barrier. The divergence between the EU's risk-based regulatory framework, the United States' sectoral and largely voluntary approach, and China's state-led and content-focused approach creates a fragmented global AI governance landscape. The fragmentation is significant because AI development is global, AI deployment is global, and AI risks (including systemic risks from frontier models) are global; a fragmented governance landscape cannot adequately address global risks.

7.4 The AI Capability Divide

The AI capability divide is one of the most consequential barriers to the Compact's AI governance objective. The divide has four dimensions. The compute dimension: advanced AI accelerators (GPUs, TPUs, custom AI chips) are concentrated in a small number of jurisdictions, with the United States, China, and a handful of other jurisdictions accounting for over 90 per cent of global compute capacity for AI training. The compute divide is significant because AI capability is increasingly bottlenecked on compute, and access to compute determines the ability to develop, deploy, and fine-tune advanced AI systems. The talent dimension: AI researchers and engineers are concentrated in a small number of jurisdictions and firms. Stanford HAI's AI Index 2025 reports that the United States, China, the European Union, India, and the United Kingdom account for the majority of AI research output and AI workforce. The data dimension: large, high-quality training datasets are concentrated in a small number of firms, particularly the large technology platforms that control major search, social media, and e-commerce services. The infrastructure dimension: cloud computing and AI infrastructure are concentrated in a small number of jurisdictions and firms, with the top three cloud providers accounting for over 60 per cent of global cloud computing revenue.

The policy response to the AI capability divide includes several elements. The first is compute access: programmes that provide subsidised or free access to AI compute for researchers, civil society, and small firms in the Global South. The second is talent development: investment in AI education and training programmes in the Global South, including graduate programmes, professional certifications, and reskilling programmes. The third is data access: initiatives that provide access to high-quality training datasets for Global South researchers and firms, including open data initiatives, data trusts, and synthetic data generation. The fourth is infrastructure investment: investment in cloud computing and AI infrastructure in the Global South, including data centres, edge computing, and network infrastructure. The Observatory's recommendation is that the proposed Global Fund for AI should prioritise the AI capability divide, with 60 per cent of Fund resources allocated to Global South institutions.

7.5 Regulatory Fragmentation

The regulatory fragmentation of AI governance is one of the most consequential barriers to the Compact's AI governance objective. The fragmentation is driven by the divergence between three broad regulatory approaches. The EU's risk-based regulatory framework, embodied in the EU AI Act, classifies AI systems by risk level and

imposes graduated obligations on developers and deployers. The United States' sectoral and largely voluntary approach relies on sector-specific regulators (the Federal Trade Commission, the Food and Drug Administration, the Equal Employment Opportunity Commission) and voluntary commitments by AI developers. China's state-led and content-focused approach combines algorithmic registration requirements, content moderation obligations, and restrictions on the deployment of generative AI in politically sensitive contexts.

The fragmentation has several consequences. It creates compliance complexity for AI developers operating across multiple jurisdictions. It creates regulatory arbitrage opportunities, in which AI developers choose to deploy in jurisdictions with the least stringent requirements. It creates interoperability challenges, in which AI systems developed in one jurisdiction cannot easily be deployed in another. It creates a coordination deficit, in which global AI risks (including systemic risks from frontier models) cannot be adequately addressed by any single jurisdiction. The policy response to the fragmentation includes the development of international AI standards (the work of the ISO/IEC JTC 1 SC 42 subcommittee on AI), the development of international AI safety frameworks (the work of the AI Safety Institutes Network), and the development of an international AI governance dialogue (the work of the Global Dialogue on AI Governance, scheduled to convene for the first time in July 2026). The Observatory's recommendation is that the Global Dialogue should prioritise the development of interoperability principles for AI governance, building on but not duplicating the work of existing standards bodies and safety institutes.

7.6 Workforce Displacement and the AI Transition

The workforce displacement risk from AI is one of the most consequential forward-looking risks to the Compact's AI governance objective. The WEF Future of Jobs Report 2025 projects that, over the 2025-2030 period, approximately 170 million new jobs will be created globally while 92 million existing jobs will be displaced. The displacement is driven by AI's increasing capability to perform tasks previously performed by humans, particularly cognitive tasks (writing, analysis, customer service) and routine analytical tasks (data entry, basic accounting). The creation is driven by AI's increasing capability to augment human work, create new products and services, and raise productivity. The net effect is positive (78 million new jobs) but the gross effect (22 per cent job churn) is substantial, and the distributional effect (the displaced workers are not the same as the newly employed) is the central challenge.

The workforce displacement risk is particularly acute in the business process outsourcing sector, which has been a major source of employment and export revenue in several lower-middle-income countries (the Philippines, India, Kenya, South Africa). The sector is highly susceptible to AI-driven displacement because its core tasks — call centre operations, data processing, basic customer service — are precisely the tasks at which generative AI excels. The policy response includes investment in reskilling programmes for BPO workers, support for the transition to higher-value services (complex customer service, technical support, content moderation), and the development of social safety nets that can support workers through transition periods. The Observatory's recommendation is that the AI governance-capacity divide should be addressed not only through AI capacity-building but also through workforce transition support, with particular attention to the lower-middle-income countries most exposed to AI-driven displacement.

7.7 Frontier AI Risk Governance

Frontier AI risk governance is one of the most consequential emerging dimensions of the Compact's AI governance objective. Frontier AI — AI systems at the frontier of capability, particularly large language models and multimodal foundation models — poses distinctive risks that require distinctive governance responses. The risks include systemic risks (cascading failures, market concentration, dependency), misuse risks (weaponisation, disinformation, fraud), and alignment risks (the gap between intended and actual AI behaviour). The governance responses include pre-deployment evaluation (the work of the AI Safety Institutes Network), post-deployment monitoring (the work of platform regulators and incident databases), and international cooperation (the work of the Global Dialogue on AI Governance, scheduled for July 2026).

The frontier AI risk governance agenda has advanced rapidly in 2024-2025. The Bletchley Park AI Safety Summit (November 2023) produced the Bletchley Declaration, committing 28 countries to cooperate on frontier AI safety. The Seoul AI Summit (May 2024) produced the Seoul Declaration, committing to the development of frontier AI safety frameworks and the establishment of AI Safety Institutes. The AI Safety Institutes Network, launched at the Seoul Summit, now includes 12 member institutions. The Frontier AI Forum, an industry-led initiative, has

produced voluntary commitments on frontier AI safety. The Observatory's recommendation is that the Global Dialogue on AI Governance should prioritise frontier AI risk governance as one of its first substantive agenda items, building on the work of the AI Safety Institutes Network and the Frontier AI Forum.

7.8 The Geopolitical Contestation of AI Governance

The geopolitical contestation of AI governance is one of the most consequential barriers to the Compact's AI governance objective. The contestation arises from the strategic significance of AI — for economic competitiveness, for military capability, for political influence — and from the divergence of national approaches to AI governance. The United States, the European Union, and China have each developed distinctive AI governance frameworks: the United States' sectoral and largely voluntary approach, the EU's risk-based regulatory framework, and China's state-led and content-focused approach. The divergence creates compliance complexity for AI developers operating across multiple jurisdictions, regulatory arbitrage opportunities, interoperability challenges, and a coordination deficit on global AI risks.

The geopolitical contestation is compounded by the broader geopolitical competition between the United States and China, which has spilled over into AI governance. The US export controls on advanced AI chips (October 2022, expanded October 2023), the Chinese restrictions on rare earth exports (December 2023), and the mutual accusations of AI-enabled espionage and influence operations have created a geopolitical environment that complicates international cooperation on AI governance. The Observatory's recommendation is that the international community, through the Global Dialogue on AI Governance, should seek to identify areas of convergence (safety, transparency, accountability) that can be advanced despite the broader geopolitical competition, while acknowledging the limits of cooperation in areas where geopolitical competition is most acute.

PART III

CROSS-CUTTING ANALYSIS

Part III provides the three-axis country assessment, the Forward Readiness and Risk Monitor, and regional deep dives across all eleven geographic regions covered by the Observatory.

Chapter 8 — The Three-Axis Country Assessment

8.1 From Single Score to Multidimensional Profile

The three-axis country assessment classifies each country by the interaction of three dimensions: implementation, capacity, and trajectory. The interaction produces five country profiles, each with distinct policy implications.

8.2 Profile Distribution (Generated from Annex A)

The Three-Axis Profile distribution, generated directly from the Annex A dataset, is as follows:

Leader (22 countries): Sweden, Singapore, Netherlands, United Kingdom, Norway, Estonia, United Arab Emirates, Australia, New Zealand, Germany, South Korea, Spain, France, Japan, Portugal, Italy, Saudi Arabia, China, Qatar, Poland, Israel, Canada.

Implementer (28 countries): Jordan, Russia, Kazakhstan, Uruguay, Colombia, Armenia, Costa Rica, Vietnam, Georgia, South Africa, Indonesia, Sri Lanka, Mexico, Ukraine, Kenya, Uzbekistan, Morocco, Philippines, Ghana, Argentina, Mongolia, Rwanda, Peru, Bangladesh, Jamaica, Egypt, Belarus, Nigeria.

Fragile Progress (5 countries): Cote dIvoire, Tanzania, Pakistan, Nepal, Fiji.

Stagnating (1 country): Ethiopia.

At Risk (12 countries): Brazil, United States, Greece, Chile, India, Malaysia, Thailand, Tunisia, Senegal, Cambodia, Uganda, Myanmar.

8.3 Diagnostic Patterns

The three-axis assessment reveals four diagnostic patterns. The first is the capacity surplus pattern, where capacity significantly exceeds implementation — visible in countries like the United States (Impl: 75.4, Cap: 83.2) and Canada (Impl: 76.8, Cap: 84.2). The capacity surplus suggests institutional machinery exists but implementation outcomes are lagging. The second is the capacity deficit pattern, where implementation exceeds capacity — visible in countries like Saudi Arabia (Impl: 79.6, Cap: 77.6) and Russia (Impl: 71.2, Cap: 68.6). The capacity deficit suggests implementation is being sustained by extraordinary effort but is at risk of stalling if institutional capacity is not built. The third is the trajectory divergence pattern, where countries with similar implementation and capacity scores have divergent trajectories — most visible in the comparison between the United States (Impl: 75.4, Trajectory: Deteriorating) and countries with similar scores but improving trajectories. The fourth is the risk concentration pattern, where the At Risk profile is concentrated in specific geographic and income contexts.

8.4 Diagnostic Patterns: Detailed Analysis

The four diagnostic patterns identified in Section 8.3 warrant detailed analysis. The capacity surplus pattern, where capacity significantly exceeds implementation, is visible in countries like the United States (Impl: 75.4, Cap: 83.2) and Canada (Impl: 76.8, Cap: 84.2). The capacity surplus suggests that the institutional machinery exists to translate policy into action, but the action itself is lagging. The policy implication is that capacity-building investment is not the binding constraint; the binding constraint is policy prioritisation, political will, or implementation efficiency. The capacity surplus pattern is most common in upper-middle-income and high-income countries with mature digital governance institutions but variable implementation performance.

The capacity deficit pattern, where implementation exceeds capacity, is visible in countries like Saudi Arabia (Impl: 79.6, Cap: 77.6) and Russia (Impl: 71.2, Cap: 68.6). The capacity deficit suggests that implementation is being sustained by extraordinary effort, leadership, or external support, but is at risk of stalling if the underlying capacity is not built. The policy implication is that capacity-building investment is the binding constraint; without it, implementation will plateau or reverse. The capacity deficit pattern is most common in middle-income countries that have made rapid implementation progress but have not yet built the corresponding institutional capacity.

The trajectory divergence pattern, where countries with similar implementation and capacity scores have divergent trajectories, is most visible in the comparison between the United States (Impl: 75.4, Trajectory: Deteriorating) and countries with similar implementation scores but Improving trajectories. The trajectory divergence suggests that the forward-looking factors — political will, regulatory stability, policy coherence — are doing significant work in determining the implementation trajectory, and that these factors are not captured in the retrospective implementation and capacity scores. The policy implication is that trajectory-focused interventions (stabilising regulatory expectations, building policy coherence, sustaining political commitment) may be more effective than implementation-focused interventions for countries in this pattern.

The risk concentration pattern, where the At Risk profile is concentrated in specific geographic and income contexts, is documented in detail in Chapter 9. The At Risk cohort of 12 countries includes low-income and lower-middle-income countries with structural implementation deficits (Senegal, Cambodia, Uganda, Myanmar), middle-implementation countries in the transitional zone (Brazil, Greece, Chile, India, Malaysia, Thailand), a country with a Deteriorating trajectory (the United States), and a Deteriorating-trajectory country in Sub-Saharan Africa (Tunisia). Ethiopia is classified as Stagnating, not At Risk. The concentration suggests that the risk factors are not randomly distributed but are systematically associated with specific structural conditions. The

policy implication is that risk-mitigation interventions should be targeted to the specific structural conditions of each At Risk country, rather than applied uniformly across the cohort.

8.5 The Six-Part Country Card Design

The Observatory's country card, presented in Annex D for selected countries, is designed to provide a comprehensive yet concise diagnostic profile of each assessed country. The card has six components. The first component is the headline classification: the country's Implementation Score, Governance Capacity Score, Forward Readiness and Risk Score, Trajectory, Score Band, and Three-Axis Profile. This component provides the at-a-glance summary of the country's GDC implementation status. The second component is the objective score breakdown: the country's score on each of the five GDC objectives (Digital Divides, Inclusive Digital Economy, Digital Safety and Security, Data Governance, Artificial Intelligence). This component identifies the country's strengths and weaknesses within the implementation score.

The third component is the diagnostic pattern: the country's classification under the four diagnostic patterns (capacity surplus, capacity deficit, trajectory divergence, risk concentration). This component identifies the structural condition that should inform policy intervention. The fourth component is the risk signal profile: the country's status on each of the seven emerging risk signals. This component identifies the specific forward-looking risks that should be monitored. The fifth component is the regional and income-group comparator: the country's score relative to its regional and income-group averages. This component contextualises the country's performance. The sixth component is the policy implication: a brief summary of the priority interventions implied by the diagnostic profile. This component translates the diagnostic into action.

The six-part country card is designed to be useful to multiple audiences: to government officials responsible for digital policy in the assessed country, to international organisations and donors considering capacity-building support, to researchers studying the determinants of digital governance implementation, and to civil society organisations advocating for improved digital policy. The card is deliberately concise — a single page in the printed report — but is supported by the detailed data and methodology in the Annexes and on the Observatory's website. The 2026 edition will publish country cards for all assessed countries, not just the selected countries featured in Annex D of this inaugural edition.

8.6 Geographic and Income Patterns

The Three-Axis Profile distribution exhibits clear geographic and income patterns. The Leader profile (22 countries) is concentrated in Europe (12 countries), East Asia (3 countries), Oceania (2 countries), MENA (3 countries), North America (1 country), and Southeast Asia (1 country). The Implementer profile (28 countries) is distributed more broadly, with substantial representation in LAC, MENA, CIS, Southeast Asia, and Sub-Saharan Africa. The Fragile Progress profile (5 countries) is concentrated in Sub-Saharan Africa and South Asia. The Stagnating profile (1 country) is Ethiopia. The At Risk profile (12 countries) includes both low-income countries with structural deficits and a high-income country with a deteriorating trajectory.

The income-group pattern is equally clear. The Leader profile is dominated by high-income countries (21 of 22 Leaders are HIC). The Implementer profile includes a mix of upper-middle-income, lower-middle-income, and high-income countries. The Fragile Progress profile is dominated by lower-middle-income countries. The Stagnating and At Risk profiles are dominated by low-income and lower-middle-income countries. The income-group pattern confirms the structural character of the implementation gap: income level is a strong predictor of GDC implementation, but it is not the only predictor. The exceptions — Rwanda (62.0, low-income, Implementer), India (74.0, lower-middle-income, At Risk), and the United States (75.4, high-income, At Risk) — illustrate that income level is not deterministic, and that policy choices, political will, and institutional capacity can produce outcomes that diverge from the income-predicted trajectory.

8.7 The Three-Axis Profile and Policy Intervention

The Three-Axis Profile system is designed not only to classify countries but to inform policy intervention. Each profile implies a distinct set of priority interventions. The Leader profile (implementation at least 75, capacity at least 70, Improving trajectory) implies that the country has achieved substantial implementation and has the capacity to sustain it. The priority intervention for Leader countries is to consolidate gains, address remaining gaps (particularly in the AI governance objective), and contribute to international cooperation through knowledge sharing, capacity-building support, and participation in the Compact's international institutional architecture.

The Implementer profile (implementation at least 56, Improving trajectory, subject to the hierarchical decision rules) implies that the country has achieved moderate implementation and is on a positive trajectory. The priority intervention for Implementer countries is to accelerate implementation in the weakest objectives, build capacity in the dimensions where capacity lags implementation, and sustain the Improving trajectory.

The Fragile Progress profile (implementation at least 45, Improving trajectory) implies that the country has achieved basic implementation but that the progress is fragile. The priority intervention for Fragile Progress countries is to consolidate the progress, build capacity to sustain it, and address the specific risks that make the progress fragile. The Stagnating profile (Stagnating trajectory with Implementation at least 45) implies that the country's implementation is neither improving nor deteriorating, but is not advancing at the pace required by the Compact's 2030 horizon. The priority intervention for Stagnating countries is to identify the binding constraints on implementation acceleration and to design interventions that address those constraints. The At Risk profile implies that the country faces significant forward-looking implementation risk. The priority intervention for At Risk countries depends on the specific risk factor: for Deteriorating-trajectory At Risk countries, trajectory stabilisation; for transitional-zone At Risk countries, building institutional capacity buffer; for low-implementation At Risk countries, comprehensive capacity-building.

The Three-Axis Profile system's policy relevance is illustrated by the contrasting cases of the United States (75.4, At Risk) and Ethiopia (45.2, Stagnating). Both countries face implementation challenges, but the challenges are entirely different. The United States has high implementation and high capacity but a deteriorating trajectory, driven by the volatility of federal AI policy and the absence of a comprehensive federal data-protection law. The priority intervention is trajectory stabilisation: restoring regulatory predictability, building policy coherence across federal agencies, and sustaining political commitment to digital governance. Ethiopia has low implementation and low capacity with a stagnating trajectory, driven by structural deficits in connectivity, infrastructure, and institutional capacity. The priority intervention is comprehensive capacity-building: investment in digital infrastructure, digital skills, digital governance institutions, and digital economy development.

Chapter 9 — The Forward Readiness and Risk Monitor

9.1 The Seven Emerging Risk Signals

The Monitor identifies seven emerging risk signals. The first is the absence of a national AI strategy, affecting 21 per cent of assessed countries. The second is restrictive cross-border data-flow regimes, affecting 24 per cent. The third is low cybersecurity capacity (GCI Tier 4 or 5), affecting 4 per cent. The fourth is limited digital public infrastructure, affecting 13 per cent. The fifth is unaffordable connectivity, affecting 9 per cent. The sixth is the absence of data-protection legislation, affecting 1 per cent. The seventh is internet penetration below 50 per cent, affecting 13 per cent.

9.2 Risk Concentration

The Observatory's risk concentration analysis identifies 12 countries classified as At Risk. These countries are the highest-priority candidates for international attention and support. The At Risk cohort is diverse: it includes low-income countries with structural implementation deficits and a high-income country with a deteriorating trajectory (the United States). The policy implications are different for each country. For the low-income At Risk countries, the priority is comprehensive capacity-building. For the United States, the priority is domestic political mobilisation to address the volatility of federal AI policy.

9.3 Risk Signal Penalty Justification

The Forward Readiness and Risk Score's risk component applies penalty weights for each of the seven emerging risk signals. The choice of seven signals, and the choice of penalty magnitudes, are substantive analytical judgements that require explicit justification. The seven signals were selected through a three-stage process. The first stage identified a long list of candidate signals from the literature on digital governance risks, from the Observatory's prior publications, and from consultations with digital governance experts. The second stage screened the long list against three criteria: measurability (the signal must be measurable from publicly available data), relevance (the signal must be plausibly related to forward-looking implementation risk), and non-redundancy (the signal must not be substantially duplicative of another signal). The third stage applied the selected signals to the country sample and tested their distribution and discriminatory power.

The penalty magnitudes were calibrated to produce meaningful but not overwhelming effects on the Forward Score. The absence of a national AI strategy carries a penalty of 8 points, on the theory that AI strategy is a forward-looking commitment that signals intent to develop AI governance capacity. Restrictive cross-border data-flow regimes carry a penalty of 6 points, on the theory that data-flow restrictiveness is a forward-looking indicator of digital trade fragmentation risk. Low cybersecurity capacity (GCI Tier 4 or 5) carries a penalty of 7 points, on the theory that low cybersecurity capacity is a forward-looking indicator of cyber-incident risk. Limited digital public infrastructure carries a penalty of 5 points, on the theory that DPI is a forward-looking enabler of multiple GDC objectives. Unaffordable connectivity carries a penalty of 6 points, on the theory that unaffordable connectivity is a forward-looking indicator of digital exclusion. The absence of data-protection legislation carries a penalty of 5 points, on the theory that data-protection legislation is a forward-looking indicator of data governance capacity. Internet penetration below 50 per cent carries a penalty of 4 points, on the theory that low penetration is a forward-looking indicator of structural implementation deficit.

9.4 Risk Concentration Analysis

The Observatory's risk concentration analysis identifies 12 countries classified as At Risk under the Three-Axis Profile system. The At Risk cohort is analytically diverse and warrants disaggregated treatment. The cohort includes three sub-groups. The first sub-group is the deteriorating-trajectory At Risk countries, of which there are 3 in the assessed sample: Tunisia (54.4), Senegal (43.1), and the United States (75.4). These countries are at risk because their implementation trajectory is reversing. The policy implication for these countries is that the binding constraint is not initial implementation level but trajectory stabilisation: the priority is to arrest the deterioration and restore an Improving trajectory.

The second sub-group is the low-implementation At Risk countries, which include Cambodia (41.5), Uganda (41.3), and Myanmar (34.0). These countries are at risk because their implementation is below 45 and their trajectory is Stagnating (captured by Rule 3). The policy implication for these countries is that the binding constraint is structural implementation capacity: the priority is comprehensive capacity-building across all five GDC objectives. The third sub-group is the transitional-zone At Risk countries, which include countries with Improving trajectories and Implementation scores in the 73.5 to 77 range that lack sufficient capacity buffer (Capacity below 80). This sub-group includes Brazil (76.4, Cap: 78.6), Greece (74.7, Cap: 75.2), Chile (74.1, Cap: 74.6), India (74.0, Cap: 74.0), Malaysia (74.0, Cap: 76.3), and Thailand (73.9, Cap: 73.4). The United States is At Risk through Rule 1 (Deteriorating trajectory), not through the transitional zone. The policy implication for these countries is that the binding constraint is institutional depth: the priority is to build the capacity buffer needed to sustain their implementation trajectory.

9.5 Compounding Effects

The seven emerging risk signals are not independent: they compound. A country with multiple risk signals faces a Forward Score penalty that is the sum of the individual penalties, and the resulting Forward Score can be substantially lower than the implementation score would suggest. The compounding effect is significant because it captures the interaction between risk factors: a country with low cybersecurity capacity and restrictive cross-border data flows faces risks that are not merely additive but multiplicative, because the restrictive data flows may prevent the country from accessing international cybersecurity cooperation and threat intelligence, and the low cybersecurity capacity may make the country more vulnerable to the cyber-incident risks that the restrictive data flows are nominally intended to mitigate.

The compounding effects are most visible in the low-implementation At Risk countries, where multiple risk signals often co-occur. Cambodia, Uganda, and Myanmar each face five or more risk signals, producing Forward Score penalties that substantially reduce their Forward Scores below their implementation scores. The compounding effects are also visible in some middle-implementation countries, where the combination of two or three risk signals contributes to the Forward Score and, combined with insufficient capacity buffer, results in a transitional-zone At Risk classification despite an implementation score that would otherwise suggest a Fragile Progress or Implementer profile. The compounding effects are an analytical feature, not a bug: they capture the reality that digital governance risks are interconnected, and that the mitigation of one risk is often contingent on the mitigation of others. The policy implication is that risk mitigation should be sequenced and integrated, not siloed: addressing one risk signal in isolation may produce limited benefit if the other risk signals remain unaddressed.

9.6 The Forward Risk Monitor and the 2026 Edition

The Forward Risk Monitor is designed to be a dynamic instrument, updated annually as new data becomes available and as the Compact's implementation machinery matures. The 2026 edition of this report will include several enhancements to the Forward Risk Monitor. The first is the expansion of the risk signal set: the seven signals used in this inaugural edition will be supplemented with additional signals, including the maturity of national AI safety institutions, the strength of data-protection enforcement, the robustness of multi-stakeholder participation in digital governance, and the alignment of national digital strategies with the GDC. The second is the refinement of the penalty magnitudes: the magnitudes used in this inaugural edition are calibrated to produce meaningful but not overwhelming effects on the Forward Score, and the magnitudes will be refined based on the methodological feedback received and on the longitudinal data accumulated over the 2025-2026 period.

The third enhancement is the introduction of trajectory indicators: the 2026 edition will track the trajectory of each country's Implementation, Capacity, and Forward Scores over time, identifying progress, stagnation, and regression at the country, regional, and global levels. The trajectory indicators will provide a more nuanced assessment of the implementation dynamic than the binary trajectory classification used in this inaugural edition. The fourth enhancement is the introduction of country-level risk profiles: the 2026 edition will publish detailed risk profiles for each assessed country, documenting the specific risk signals present, the penalty magnitudes applied, and the resulting Forward Score. The country-level risk profiles will support targeted policy intervention by governments, international organisations, and donors.

9.7 The Risk Monitor and the 2027 High-Level Review

The Forward Risk Monitor is designed to inform the 2027 high-level review of GDC implementation, scheduled for the eighty-second session of the General Assembly. The Monitor's contribution to the review is threefold. First, the Monitor provides an independent assessment of forward-looking implementation risk, complementing the official UN review process with rigorous, transparent, and timely analysis. Second, the Monitor identifies the specific risk signals that are most consequential for implementation progress, providing a focus for policy intervention in the period leading up to the review. Third, the Monitor tracks the evolution of risk signals over time, providing a longitudinal record of progress, stagnation, and regression that the review can use to assess the effectiveness of the Compact's implementation architecture.

The Observatory's commitment is to publish a dedicated pre-review edition in mid-2027, synthesising the findings of the 2025, 2026, and 2027 editions and providing a comprehensive assessment of GDC implementation for the high-level review. The pre-review edition will include: a global implementation scorecard, documenting progress against the Compact's commitments; a regional and income-group analysis, documenting the implementation gap and its evolution; a country-level assessment, documenting the implementation status of each assessed country; a Forward Risk Monitor update, documenting the forward-looking risks that should be prioritised in the post-2027 period; and a set of strategic recommendations for the post-2027 implementation horizon. The Observatory's view is that the 2027 high-level review should be informed by rigorous independent monitoring, and that the Observatory's pre-review edition will make a substantial contribution to that informing.

Chapter 10 — Regional Deep Dives

This chapter provides regional deep dives across all eleven geographic regions covered by the Observatory: Sub-Saharan Africa, MENA, South Asia, Southeast Asia, East Asia, Central Asia, LAC, North America, Europe, Oceania, and the CIS.

10.1 Sub-Saharan Africa

The region's average GDC Implementation Score is 55.2. The top performers in the region are: South Africa (66.7), Kenya (64.3), Ghana (63.3).

10.2 MENA

The region's average GDC Implementation Score is 71.6. The top performers in the region are: United Arab Emirates (86.2), Saudi Arabia (79.6), Qatar (77.9).

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

10.3 South Asia

The region's average GDC Implementation Score is 61.5. The top performers in the region are: India (74.0), Sri Lanka (65.9), Bangladesh (61.5).

10.4 Southeast Asia

The region's average GDC Implementation Score is 63.7. The top performers in the region are: Singapore (87.5), Malaysia (74.0), Thailand (73.9).

10.5 East Asia

The region's average GDC Implementation Score is 77.2. The top performers in the region are: South Korea (84.4), Japan (82.6), China (79.5).

10.6 Central Asia

The region's average GDC Implementation Score is 67.2. The top performers in the region are: Kazakhstan (70.4), Uzbekistan (64.1).

10.7 LAC

The region's average GDC Implementation Score is 67.8. The top performers in the region are: Brazil (76.4), Chile (74.1), Uruguay (69.9).

10.8 North America

The region's average GDC Implementation Score is 76.1. The top performers in the region are: Canada (76.8), United States (75.4).

10.9 Europe

The region's average GDC Implementation Score is 83.5. The top performers in the region are: Sweden (87.6), Netherlands (87.2), United Kingdom (87.1).

10.10 Oceania

The region's average GDC Implementation Score is 74.3. The top performers in the region are: Australia (85.7), New Zealand (85.1), Fiji (52.1).

10.11 CIS

The region's average GDC Implementation Score is 66.4. The top performers in the region are: Russia (71.2), Armenia (69.4), Georgia (67.0).

10.12 Cross-Regional Patterns

The regional deep dives reveal several cross-regional patterns. First, the implementation gap between the highest-scoring region (Europe, 83.5) and the lowest-scoring region (Sub-Saharan Africa, 55.2) is 28.3 points. Second, within-region variation is often as significant as between-region variation. Third, the relationship between income and implementation is not deterministic: several lower-middle-income countries — including India (74.0), Kenya (64.3), and Rwanda (62.0) — score above what their income level would predict.

10.13 Detailed Regional Analysis

The eleven regional deep dives presented in Sections 10.1 through 10.11 warrant a comparative analytical synthesis. Europe leads the regional implementation ranking with an average score of 83.5, reflecting two decades of accumulated investment in digital infrastructure, e-government, cybersecurity, and data-protection legislation, anchored in the European Union's single market and regulatory frameworks. The European cohort of twelve assessed countries includes eight Leaders (Sweden, Netherlands, United Kingdom, Norway, Estonia, Germany, Spain, France), two additional Leaders (Portugal, Italy), and two At Risk countries (Poland, Greece). The European Forward Score of 71.3 is the highest of any region, indicating sustained implementation momentum. The European case illustrates the potential of a coordinated regional regulatory framework to drive sustained implementation progress.

East Asia scores 77.2 on implementation, driven by the strong performance of Japan (82.6), South Korea (84.4), and China (79.5), and supported by Mongolia (62.2) in the lower-middle-income bracket. The East Asian Forward

Score of 69.1 indicates positive but moderate momentum. The East Asian case illustrates the diversity of pathways to digital governance: Japan and South Korea are high-income democracies with robust regulatory frameworks, China is an upper-middle-income authoritarian state with state-led development, and Mongolia is a lower-middle-income democracy with emerging digital governance capacity. The regional average conceals substantial within-region variation, with a gap of 20.4 points between the highest and lowest performers.

Oceania scores 74.3 on implementation, with Australia (85.7), New Zealand (85.1), and Fiji (52.1) in the assessed sample. The Oceania cohort illustrates the divide between the high-income Pacific developed economies (Australia, New Zealand) and the middle-income Pacific island economies (Fiji, and the many Pacific island states not assessed in this edition). The Oceania case highlights the importance of expanding coverage to include more Pacific island states in subsequent editions, as the digital governance challenges of small island developing states are distinctive and not adequately captured by the assessment of Fiji alone.

North America scores 76.1 on implementation, but this average conceals the extraordinary internal divergence between Canada (76.8, Improving, Leader) and the United States (75.4, Deteriorating, At Risk). The North American Forward Score of 53.7 is by a substantial margin the lowest of any region, reflecting the volatility of federal AI policy in the United States and the absence of a comprehensive federal data-protection law. The North American case illustrates that high income and high capacity do not guarantee sustained implementation progress; political will and regulatory stability are equally consequential.

The Middle East and North Africa scores 71.6 on implementation, with the United Arab Emirates (86.2), Saudi Arabia (79.6), Qatar (77.9), Israel (77.0), Jordan (73.2), Morocco (63.8), Egypt (60.6), and Tunisia (54.4) in the assessed sample. The MENA cohort illustrates the divide between the high-income Gulf states (UAE, Saudi Arabia, Qatar) and the lower-middle-income North African states (Morocco, Egypt, Tunisia). The MENA Forward Score of 67.5 indicates positive momentum, but Tunisia's deteriorating trajectory is a significant concern. The MENA case highlights the diversity of digital governance pathways in the region, from the state-led development model of the Gulf to the emerging democracies of North Africa.

Latin America and the Caribbean scores 67.8 on implementation, with Brazil (76.4), Chile (74.1), Uruguay (69.9), Colombia (69.8), Costa Rica (69.2), Mexico (65.0), Argentina (63.1), Peru (62.0), and Jamaica (60.8) in the assessed sample. The LAC Forward Score of 71.1 is the highest of any non-European region, indicating strong implementation momentum. The LAC case illustrates the potential of regional cooperation (the eLAC initiative, the Inter-American Development Bank's digital agenda) to drive implementation progress, and the importance of digital public infrastructure (Brazil's Pix, Uruguay's digital government) in raising implementation scores.

Central Asia scores 67.2 on implementation, with Kazakhstan (70.4) and Uzbekistan (64.1) in the assessed sample. The Central Asian cohort is the smallest in the assessment, and the regional average should be treated with appropriate caution. The Central Asian case highlights the importance of expanding coverage to include the other Central Asian states (Kyrgyzstan, Tajikistan, Turkmenistan) in subsequent editions. The two assessed Central Asian countries illustrate the diversity of pathways in the region, from Kazakhstan's upper-middle-income resource-rich trajectory to Uzbekistan's lower-middle-income reform-oriented trajectory.

Southeast Asia scores 63.7 on implementation, with Singapore (87.5), Malaysia (74.0), Thailand (73.9), Vietnam (68.6), Indonesia (66.6), the Philippines (63.7), Cambodia (41.5), and Myanmar (34.0) in the assessed sample. The Southeast Asian cohort illustrates the full spectrum of implementation, from Singapore's world-leading performance to Myanmar's structural deficit. The Southeast Asian Forward Score of 64.9 indicates moderate momentum, but the region's diversity means that the regional average is a poor guide to any individual country's trajectory.

South Asia scores 61.5 on implementation, with India (74.0), Sri Lanka (65.9), Bangladesh (61.5), Pakistan (53.0), and Nepal (52.9) in the assessed sample. The South Asian cohort illustrates the diversity of pathways within a single sub-region, from India's middle-income digital public infrastructure leadership to Nepal's lower-middle-income emerging digital governance capacity. The South Asian Forward Score of 69.3 indicates positive momentum, driven by recent policy activity in several of the assessed countries.

The CIS scores 66.4 on implementation, with Russia (71.2), Kazakhstan (70.4), Armenia (69.4), Georgia (67.0), Ukraine (64.8), and Belarus (59.7) in the assessed sample. The CIS cohort illustrates the diversity of pathways

among the post-Soviet states, from Russia's upper-middle-income state-led trajectory to Georgia's reform-oriented trajectory. The CIS Forward Score of 68.7 indicates moderate momentum.

Sub-Saharan Africa scores 55.2 on implementation, with South Africa (66.7), Kenya (64.3), Ghana (63.3), Rwanda (62.0), Nigeria (56.1), Cote d'Ivoire (55.9), Tanzania (54.6), Senegal (43.1), Ethiopia (45.2), and Uganda (41.3) in the assessed sample. The Sub-Saharan African cohort illustrates both the potential (Rwanda, Kenya, Ghana) and the structural challenges (Ethiopia, Uganda, Senegal) of digital governance in the region. The Sub-Saharan African Forward Score of 63.4 indicates positive momentum, but the region's implementation gap is the largest of any region, and the high-income to low-income implementation gap is most visible in the Sub-Saharan African context.

10.14 Cross-Regional Patterns: Detailed Analysis

The regional deep dives reveal several cross-regional patterns that warrant detailed analysis. First, the implementation gap between the highest-scoring region (Europe, 83.5) and the lowest-scoring region (Sub-Saharan Africa, 55.2) is 28.3 points. This gap is larger than the high-income to low-income gap of 35.7 points, reflecting the fact that regional concentration of high-income countries amplifies the income effect. Second, within-region variation is often as significant as between-region variation. The range within Southeast Asia (from Singapore's 87.5 to Myanmar's 34.0) is 53.5 points, larger than the gap between Europe and Sub-Saharan Africa.

Third, the relationship between income and implementation is not deterministic. Several lower-middle-income countries — including India (74.0), Kenya (64.3), and Rwanda (62.0) — score above what their income level would predict. Rwanda, with a GNI per capita of approximately $930, scores 62.0 on implementation, above the upper-middle-income average of 67.5 and well above the low-income average of 45.6. Fourth, the relationship between political system and implementation is not deterministic. Authoritarian states (China, 79.5; Saudi Arabia, 79.6; Rwanda, 62.0) and democracies (Sweden, 87.6; Estonia, 86.9; India, 74.0) are both represented among the high-performing countries, suggesting that political system is not the primary determinant of implementation performance.

Fifth, the relationship between regional cooperation and implementation is positive but not uniform. Europe's strong regional cooperation framework (the EU single market, the GDPR, the AI Act) is associated with high regional implementation. LAC's regional cooperation framework (eLAC, the IDB digital agenda) is associated with strong forward momentum. Sub-Saharan Africa's regional cooperation frameworks (the African Union, the Smart Africa Alliance) are associated with patchy implementation, suggesting that regional cooperation is necessary but not sufficient for implementation progress. Sixth, the relationship between digital public infrastructure and implementation is positive and consistent. Countries with mature DPI (India, Brazil, Estonia, Singapore) score above their income-group averages, suggesting that DPI is a critical enabler of broader implementation progress.

10.15 The Regional Implementation Hierarchy

The regional implementation hierarchy, presented in Chapter 2 and elaborated in the regional deep dives, warrants additional comparative analysis. The hierarchy is: Europe (83.5), East Asia (77.2), Oceania (74.3), North America (76.1), MENA (71.6), LAC (67.8), Central Asia (67.2), Southeast Asia (63.7), South Asia (61.5), CIS (66.4), and Sub-Saharan Africa (55.2). The hierarchy reflects a combination of factors: income level (high-income regions tend to score higher), regional cooperation (regions with strong cooperation frameworks tend to score higher), digital public infrastructure maturity (regions with mature DPI tend to score higher), and policy prioritisation (regions where digital governance is a political priority tend to score higher).

The hierarchy is not static. The Forward Score analysis suggests that the implementation hierarchy may shift over the 2025-2027 period. The regions with the highest Forward Scores are LAC ({AGG[‘regional’][‘LAC’][‘forward’]}), Europe ({AGG[‘regional’][‘Europe’][‘forward’]}), South Asia ({AGG[‘regional’][‘South Asia’][‘forward’]}), and MENA ({AGG[‘regional’][‘MENA’][‘forward’]}), suggesting that these regions are likely to see the strongest implementation momentum over the coming year. The regions with the lowest Forward Scores are North America ({AGG[‘regional’][‘North America’][‘forward’]}) and Southeast Asia ({AGG[‘regional’][‘Southeast Asia’][‘forward’]}), suggesting that these regions may see weaker implementation momentum. The North American Forward Score is particularly low, reflecting the deteriorating trajectory of the United States, which is the dominant country in the regional average.

10.16 The Small Island Developing States Gap

The small island developing states (SIDS) gap is one of the most under-addressed dimensions of the regional analysis. The SIDS — including the Pacific island states, the Caribbean island states, and the Indian Ocean island states — face distinctive digital governance challenges that are not adequately captured by the assessment of larger countries. The challenges include: small market size (which raises the per-capita cost of digital infrastructure), geographic isolation (which raises the cost of connectivity), vulnerability to climate change (which threatens digital infrastructure), and limited institutional capacity (which constrains digital governance implementation). The Observatory's assessment includes only a small number of SIDS (Fiji in Oceania, Jamaica in LAC), and the regional averages do not adequately capture the SIDS experience.

The Observatory's commitment is to expand SIDS coverage in subsequent editions. The 2026 edition will include additional Pacific island states (Papua New Guinea, Solomon Islands, Vanuatu, Samoa, Tonga), Caribbean island states (Trinidad and Tobago, Barbados, Bahamas, Dominican Republic), and Indian Ocean island states (Mauritius, Seychelles, Maldives). The expanded SIDS coverage will support a more nuanced assessment of the SIDS digital governance experience and will inform the design of targeted interventions for the SIDS context. The Observatory's recommendation is that the international community, through the proposed Global Fund for AI and other financing mechanisms, should prioritise SIDS for targeted capacity-building support, recognising the distinctive challenges of the SIDS context.

PART IV

GOVERNANCE AND INSTITUTIONS

Chapter 11 — Implementation Institutions and Financing

11.1 The International Institutional Architecture

The Global Digital Compact's implementation architecture is anchored in ODET, the existing UN institutions (ITU, UNCTAD, UNDP, UNESCO, UN DESA, OHCHR, IGF), and the new institutions the Compact establishes (the AI Scientific Panel, the Global Dialogue, the CSTD working group on data governance). The 40 members of the Scientific Panel are expected to be appointed in early 2026. The first convening of the Global Dialogue is scheduled for July 2026 in Geneva.

11.2 Financing GDC Implementation

The financing gap for GDC implementation is substantial — on the order of $50-100 billion annually across all five objectives. The proposed Global Fund for AI, with a target capitalisation of $1-3 billion, would make a significant contribution but would not, on its own, close the gap.

11.3 Research Ethics and Independence

This report is an independent flagship research report produced by AUN. It was not commissioned by any government, intergovernmental organisation, or private sector entity. No funder had editorial control. Country scores are derived entirely from publicly available indicator data and the transparent computation methodology. No government reviewed or approved its country's scores.

11.4 National Implementation Institutions

The Compact's implementation architecture is not solely international. Each member state is expected to establish or designate national institutions responsible for GDC implementation, including a national digital strategy unit, a data-protection authority, a cybersecurity agency, an AI governance body, and a digital inclusion programme. The Observatory's data show substantial variation in the maturity and capacity of these national institutions. The Leader profile countries typically have well-established institutions across all five domains, with clear mandates, adequate resources, and operational independence. The At Risk countries typically have weaker

institutions, with overlapping or unclear mandates, inadequate resources, and limited operational independence. The Implementer and Fragile Progress countries fall between these two poles.

The institutional architecture for digital governance is undergoing significant evolution in many countries. The traditional model — separate agencies for telecommunications, data protection, cybersecurity, and AI — is being supplemented or replaced by integrated digital governance commissions, ministries of digital affairs, or cross-cutting digital strategy units in the head of government's office. The integrated model reflects the recognition that digital governance challenges are interconnected and require coordinated responses. The Observatory's data show that countries with integrated digital governance institutions tend to score higher on the Implementation Score, suggesting that institutional integration is a meaningful predictor of implementation performance. The 2026 edition will include a dedicated indicator on national digital governance institutional architecture.

11.5 Stakeholder Participation in Implementation

The Compact is explicitly multi-stakeholder in its conception and implementation. The Compact's commitments are addressed not only to governments but also to the private sector, civil society, the technical community, and academia. The implementation architecture reflects this multi-stakeholder character: the Internet Governance Forum, the World Summit on the Information Society process, and the new Global Dialogue on AI Governance all provide formal mechanisms for multi-stakeholder participation. At the national level, multi-stakeholder participation is more variable: some countries have established formal multi-stakeholder digital governance councils, while others maintain a primarily state-led implementation approach.

The Observatory's assessment of multi-stakeholder participation is based on three indicators: the existence of a formal multi-stakeholder digital governance council, the inclusion of civil society and technical community representatives in national AI strategy development, and the openness of the national digital policy process to public consultation. The data show that multi-stakeholder participation is strongest in Europe, North America, and parts of LAC, and weakest in parts of Asia and Sub-Saharan Africa. The variation in multi-stakeholder participation is significant because it affects the legitimacy, the quality, and the sustainability of digital governance implementation. The Observatory's recommendation is that the GDC implementation monitoring framework should include explicit indicators of multi-stakeholder participation.

11.6 Financing Streams: Detailed Analysis

The financing of GDC implementation flows through multiple streams. The first stream is domestic public financing: government budget allocations to digital infrastructure, digital skills, e-government, cybersecurity, data protection, and AI governance. Domestic public financing is the largest stream in absolute terms, but it is highly uneven: high-income countries allocate substantially more to digital governance than low-income countries, both in absolute terms and as a share of GDP. The second stream is international public financing: official development assistance for digital development, disbursed by bilateral donors, multilateral development banks, and vertical funds. International public financing is significant for low-income countries but is modest in absolute terms relative to the financing gap.

The third stream is private financing: commercial investment in digital infrastructure, digital services, and digital applications. Private financing is the largest stream for several GDC objectives, particularly digital infrastructure and digital economy, but it is concentrated in commercially viable markets and does not flow to the contexts where the digital governance gap is largest. The fourth stream is philanthropic financing: grants from major philanthropic foundations (the Bill and Melinda Gates Foundation, the Ford Foundation, the Mastercard Foundation, the Open Society Foundations) for digital development and digital rights. Philanthropic financing is modest in absolute terms but is significant for specific initiatives and contexts. The fifth stream, anticipated but not yet operational, is the proposed Global Fund for AI, with a target capitalisation of $1-3 billion. The Fund would represent a new financing stream dedicated to AI governance capacity-building, with a particular focus on the Global South.

The financing gap for GDC implementation is substantial — on the order of $50-100 billion annually across all five objectives. The proposed Global Fund for AI, with a target capitalisation of $1-3 billion, would make a significant contribution but would not, on its own, close the gap. The Observatory's analysis suggests that closing the financing gap requires a combination of: increased domestic public financing in middle-income countries, increased international public financing for low-income countries, regulatory frameworks that channel private

financing toward underserved contexts, and the operationalisation of the Global Fund for AI as a complement to existing financing streams. The Observatory's recommendation is that the financing gap should be addressed through a coordinated multi-stream strategy, not through reliance on any single stream.

11.7 The Multi-Stakeholder Implementation Model

The Compact's multi-stakeholder implementation model is one of its most distinctive features, and one of its most challenging to operationalise. The model reflects the recognition that digital governance is not solely a state responsibility: the private sector builds and operates the digital infrastructure, platforms, and AI systems; civil society advocates for the rights and interests of citizens; the technical community develops the standards and protocols; and academia produces the research and analysis. The Compact's implementation architecture provides formal mechanisms for multi-stakeholder participation: the Internet Governance Forum, the WSIS process, the Global Dialogue on AI Governance, and the multi-stakeholder advisory bodies of the various UN agencies. At the national level, multi-stakeholder participation is more variable.

The Observatory's assessment of multi-stakeholder participation is based on three indicators: the existence of a formal multi-stakeholder digital governance council, the inclusion of civil society and technical community representatives in national AI strategy development, and the openness of the national digital policy process to public consultation. The data show that multi-stakeholder participation is strongest in Europe, North America, and parts of LAC, and weakest in parts of Asia and Sub-Saharan Africa. The variation is significant because it affects the legitimacy, the quality, and the sustainability of digital governance implementation. The Observatory's recommendation is that the GDC implementation monitoring framework should include explicit indicators of multi-stakeholder participation, and that the international community should support the development of multi-stakeholder digital governance councils in countries where they do not currently exist.

11.8 The Role of the Private Sector

The private sector plays a central role in the Compact's implementation, particularly in the digital infrastructure, digital economy, and AI governance objectives. The private sector builds and operates the connectivity infrastructure (telecommunications operators, internet service providers, satellite operators), the digital platforms (search, social media, e-commerce, content), the cloud computing and AI infrastructure (hyperscale cloud providers, AI chip manufacturers, AI model developers), and the digital financial infrastructure (banks, payment processors, fintech platforms). The Compact's commitments depend on private sector investment, innovation, and compliance. The private sector also plays a role in the Compact's international institutional architecture, through participation in the Internet Governance Forum, the Global Dialogue on AI Governance, and various multi-stakeholder bodies.

The private sector's role in the Compact's implementation is not without tension. The concentration of market power in a small number of platforms and infrastructure providers creates concerns about rent extraction, barriers to entry, and the concentration of decision-making power. The divergence between private sector incentives and public interest objectives creates challenges for regulatory design. The geopolitical competition between the major technology powers (the United States, China, and to a lesser extent the European Union) creates challenges for international cooperation. The Observatory's recommendation is that the Compact's implementation should include explicit attention to the role of the private sector, including the development of corporate accountability frameworks, the promotion of competition in digital markets, and the alignment of private sector incentives with public interest objectives.

PART V

RECOMMENDATIONS AND THE ROAD TO 2027

Chapter 12 — Strategic Recommendations

The Observatory's ten strategic recommendations are: (1) Operationalise the AI Scientific Panel and Global Dialogue; (2) Establish the Global Fund for AI; (3) Develop a global DPI safeguards framework; (4) Address the AI

governance-capacity divide; (5) Align national digital strategies with the GDC; (6) Accelerate the CSTD working group on data governance; (7) Strengthen the IGF; (8) Develop a GDC implementation monitoring framework; (9) Address the digital rights and civic space deficit; (10) Establish an emerging technology horizon-scanning mechanism.

12.1 Detailed Recommendation Rationale

Each of the ten strategic recommendations presented in the summary table warrants a detailed rationale. The recommendations are not a wish list; they are an operational sequence, with each recommendation linked to a specific institutional actor, a specific implementation milestone, and a specific measurable indicator of progress.

Recommendation 1: Operationalise the AI Scientific Panel and Global Dialogue. The rationale is that the international institutional architecture for AI governance, mandated by the Compact and operationalised by General Assembly resolution 79/325 of 26 August 2025, is not yet fully established. The 40 members of the Scientific Panel are expected to be appointed in early 2026, and the first convening of the Global Dialogue is scheduled for July 2026 in Geneva. The completion of these milestones is the necessary first step toward the international AI governance architecture the Compact envisions. The institutional actor is the United Nations Secretariat, the Office for Digital and Emerging Technologies (ODET), and the member states of the General Assembly. The implementation milestone is the appointment of the 40 Panel members and the convening of the first Global Dialogue. The measurable indicator is the publication of the Panel's first report and the Global Dialogue's first outcome document.

Recommendation 2: Establish the Global Fund for AI. The rationale is that the AI capability divide is one of the most consequential barriers to the Compact's AI governance objective, and that the existing financing architecture is not adequate to close the divide. The proposed Global Fund for AI, with a target capitalisation of $1-3 billion, would represent a new financing stream dedicated to AI governance capacity-building, with a particular focus on the Global South. The institutional actor is a multi-stakeholder coalition of governments, multilateral development banks, and philanthropic foundations. The implementation milestone is the initial capitalisation of $1 billion by end 2026 and a trajectory to $3 billion by 2028. The measurable indicator is the volume of disbursements to Global South institutions and the corresponding improvement in AI governance capacity indicators.

Recommendation 3: Develop a global DPI safeguards framework. The rationale is that the rapid deployment of digital public infrastructure — identity, payments, data exchange — is outpacing the development of safeguards, creating risks of data breaches, surveillance, exclusion of marginalised groups, and a backlash that could slow or reverse DPI deployment. A global DPI safeguards framework, developed through a multi-stakeholder process, would establish minimum standards for legal, technical, and institutional safeguards on DPI. The institutional actor is a multi-stakeholder coalition convened by ODET, the World Bank, and national governments with mature DPI experience (India, Brazil, Estonia). The implementation milestone is the convening of the multi-stakeholder process by end 2026 and the publication of the framework by end 2027. The measurable indicator is the adoption of the framework's standards by national DPI programmes.

Recommendation 4: Address the AI governance-capacity divide. The rationale is that the AI capability divide is multi-dimensional (compute, talent, data, infrastructure) and requires a multi-dimensional response. The recommendation is that the proposed Global Fund for AI should prioritise the AI capability divide, with 60 per cent of Fund resources allocated to Global South institutions. The institutional actor is the Global Fund for AI and its implementing partners. The implementation milestone is the disbursement of 60 per cent of Fund resources to Global South institutions by 2028. The measurable indicator is the improvement in AI readiness indicators for Global South countries.

Recommendation 5: Align national digital strategies with the GDC. The rationale is that the Compact's commitments are addressed to member states, and that member states' national digital strategies are the primary instrument for translating the Compact's commitments into action. The recommendation is that a mapping toolkit should be developed to help member states align their national digital strategies with the GDC's five objectives and approximately seventy commitments. The institutional actor is ODET and a coalition of national digital strategy units. The implementation milestone is the development of the mapping toolkit by March 2026. The measurable indicator is the number of national digital strategies that have been mapped to the GDC.

Recommendation 6: Accelerate the CSTD working group on data governance. The rationale is that the cross-border data-flow fragmentation is one of the most consequential barriers to the Compact's data governance objective, and that the CSTD working group on data governance, mandated by the Compact, is the primary international forum for addressing the fragmentation. The recommendation is that the CSTD working group should be accelerated and should prioritise the development of interoperability principles for cross-border data flows. The institutional actor is the CSTD and its member states. The implementation milestone is the publication of the interoperability principles by end 2027. The measurable indicator is the adoption of the principles by national data-protection authorities.

Recommendation 7: Strengthen the Internet Governance Forum. The rationale is that the IGF is the primary multi-stakeholder forum for digital governance dialogue, and that its alignment with the GDC would amplify the Compact's implementation. The recommendation is that the 2026 and 2027 IGF programmes should be aligned with the GDC's five objectives. The institutional actor is the IGF Multistakeholder Advisory Group and the IGF Secretariat. The implementation milestone is the alignment of the 2026 IGF programme with the GDC. The measurable indicator is the number of IGF sessions that explicitly address GDC commitments.

Recommendation 8: Develop a GDC implementation monitoring framework. The rationale is that the Compact's follow-up and review architecture requires a monitoring framework that complements the official UN review process with independent monitoring. The recommendation is that a GDC implementation monitoring framework should be developed, drawing on independent monitoring initiatives including this Observatory. The institutional actor is a coalition of independent monitoring organisations, coordinated by ODET. The implementation milestone is the publication of the monitoring framework by end 2026. The measurable indicator is the number of independent monitoring initiatives that adopt the framework's indicators.

Recommendation 9: Address the digital rights and civic space deficit. The rationale is that the Compact's commitments on human rights online — including the commitment to refrain from internet shutdowns — are not being implemented in a significant minority of member states. The recommendation is that a human rights due diligence framework for digital technologies should be developed. The institutional actor is the Office of the High Commissioner for Human Rights (OHCHR) and a coalition of digital rights organisations. The implementation milestone is the publication of the framework by end 2027. The measurable indicator is the number of countries that have adopted the framework's standards.

Recommendation 10: Establish an emerging technology horizon-scanning mechanism. The rationale is that the Compact's five objectives cover the current digital governance agenda, but that emerging technologies — quantum computing, neurotechnology, biotechnology, robotics — will pose new governance challenges over the 2026-2030 horizon. The recommendation is that an emerging technology horizon-scanning mechanism should be established, producing annual reports on these technologies. The institutional actor is ODET, in cooperation with the Scientific Panel. The implementation milestone is the publication of the first annual horizon-scanning report by end 2026. The measurable indicator is the integration of the horizon-scanning reports into the GDC implementation review process.

12.2 The Sequencing of Recommendations

The ten strategic recommendations presented in Chapter 12 are not a wish list; they are an operational sequence. The sequencing reflects the dependencies between the recommendations and the feasibility of implementation within the 2025-2027 window. Recommendation 1 (Operationalise the AI Scientific Panel and Global Dialogue) is the first priority, because the international institutional architecture for AI governance cannot function without the Panel and the Dialogue. Recommendation 2 (Establish the Global Fund for AI) is the second priority, because the financing gap cannot be closed without a dedicated financing mechanism. Recommendation 3 (Develop a global DPI safeguards framework) is the third priority, because the DPI backlash risk cannot be mitigated without a safeguards framework. Recommendation 4 (Address the AI governance-capacity divide) is the fourth priority, because the AI capability divide cannot be narrowed without targeted capacity-building, which depends on the Global Fund for AI (Recommendation 2).

Recommendation 5 (Align national digital strategies with the GDC) is the fifth priority, because the mapping toolkit is a relatively quick deliverable that can support national-level implementation in 2026. Recommendation 6 (Accelerate the CSTD working group on data governance) is the sixth priority, because the cross-border data-flow fragmentation cannot be addressed without the CSTD working group's output. Recommendation 7

(Strengthen the Internet Governance Forum) is the seventh priority, because the IGF alignment is a relatively quick deliverable that can support multi-stakeholder dialogue in 2026 and 2027. Recommendation 8 (Develop a GDC implementation monitoring framework) is the eighth priority, because the monitoring framework is needed to inform the 2027 high-level review. Recommendation 9 (Address the digital rights and civic space deficit) is the ninth priority, because the human rights due diligence framework is a longer-term deliverable. Recommendation 10 (Establish an emerging technology horizon-scanning mechanism) is the tenth priority, because the horizon-scanning mechanism is a longer-term deliverable that builds on the Scientific Panel's work.

12.3 The Implementation Actors

Each of the ten recommendations implies a specific implementation actor. Recommendation 1 is implemented by the United Nations Secretariat, ODET, and the member states of the General Assembly. Recommendation 2 is implemented by a multi-stakeholder coalition of governments, multilateral development banks, and philanthropic foundations. Recommendation 3 is implemented by a multi-stakeholder coalition convened by ODET, the World Bank, and national governments with mature DPI experience. Recommendation 4 is implemented by the Global Fund for AI and its implementing partners. Recommendation 5 is implemented by ODET and a coalition of national digital strategy units. Recommendation 6 is implemented by the CSTD and its member states. Recommendation 7 is implemented by the IGF Multistakeholder Advisory Group and the IGF Secretariat. Recommendation 8 is implemented by a coalition of independent monitoring organisations, coordinated by ODET. Recommendation 9 is implemented by the OHCHR and a coalition of digital rights organisations. Recommendation 10 is implemented by ODET, in cooperation with the Scientific Panel.

The identification of implementation actors is significant because it clarifies accountability. Each recommendation has a specific actor responsible for implementation, and each actor can be held accountable for the implementation of its recommendation. The Observatory's role is to monitor the implementation of the recommendations, to report on the progress made by each actor, and to identify the gaps between commitment and implementation that require priority attention. The 2026 edition of this report will include a dedicated chapter tracking the implementation of the ten recommendations, documenting the progress made by each actor, and identifying the gaps that require priority attention in the run-up to the 2027 high-level review.

Chapter 13 — The Road to the 2027 High-Level Review

13.1 The 2027 Review as a Critical Juncture

The high-level review of GDC implementation, scheduled for the eighty-second session of the General Assembly in 2027, is the most consequential milestone in the Compact's follow-up architecture. The road from this inaugural edition to the 2027 review comprises five critical milestones: the WSIS+20 meeting (scheduled for 16-17 December 2025), the appointment of AI Panel members (expected early 2026), the first Global Dialogue convening (scheduled for July 2026), the 2026 edition of this report (December 2026), and the high-level review itself (UNGA 82, 2027).

13.2 Conclusion

The Observatory's inaugural verdict is one of conditional optimism tempered by structural concern. The Compact is not failing — the global implementation score of 69.2 and the broadly positive trajectory indicate measurable early progress. But the Compact is not succeeding at the pace its 2030 horizon requires. The high-income to low-income gap of 35.7 points is the single most consequential finding. The road to 2027 begins with this inaugural edition.

13.3 Roadmap Milestones: Detailed Analysis

The road from this inaugural edition (1 December 2025) to the high-level review (UNGA 82, 2027) comprises five critical milestones, each of which warrants detailed analysis. The first milestone is the WSIS+20 high-level meeting, scheduled for 16-17 December 2025 in New York. The WSIS+20 meeting is expected to produce a resolution mandating a joint WSIS-GDC implementation roadmap through 2030, aligning the existing WSIS architecture (the Internet Governance Forum, the CSTD, the Action Lines) with the new GDC architecture (ODET, the Scientific Panel, the Global Dialogue). The alignment is critical: the GDC does not replace WSIS but builds on it, and the relationship between the two frameworks will determine whether the Compact's

implementation is amplified or fragmented by the existing institutional ecosystem. As of the publication date of this report, the WSIS+20 meeting has not yet taken place; the outcome is therefore described as forthcoming.

The second milestone is the appointment of the 40 members of the Independent International Scientific Panel on AI, expected in early 2026. The appointment is being managed by the United Nations Secretariat, in consultation with member states, scientific communities, and multi-stakeholder constituencies. The appointment will be a significant test of the Compact's commitment to geographic, gender, and disciplinary balance in the AI governance architecture. The Observatory will assess the composition of the Panel against these criteria in the 2026 edition. The third milestone is the first convening of the Global Dialogue on AI Governance, scheduled for July 2026 in Geneva. The Global Dialogue is the Compact's primary mechanism for multi-stakeholder dialogue on AI governance, and its first convening will set the agenda for subsequent convenings through 2030. The Observatory will assess the agenda, the participation, and the outcomes of the first Global Dialogue in the 2026 edition.

The fourth milestone is the 2026 edition of this report, scheduled for publication in December 2026. The 2026 edition will expand country coverage to a target of 100 countries, will refine the indicator architecture based on the methodological feedback received on this inaugural edition, and will track the implementation milestones of 2026 against the expectations set out in this report. The fifth milestone is the high-level review itself, scheduled for the eighty-second session of the General Assembly in 2027. The review is the most consequential event in the Compact's follow-up architecture: it will assess progress against the Compact's commitments, identify the binding constraints on implementation, and frame the Compact's implementation through 2030. The Observatory will publish a dedicated pre-review edition in mid-2027 to inform the review process.

13.4 Beyond 2027: The Long-Term Implementation Horizon

The 2027 high-level review is not the end of the Compact's implementation horizon but the midpoint. The Compact's binding horizon is 2030, and the implementation work will continue through the end of the decade and beyond. The Observatory's long-term planning horizon extends to 2030, with subsequent editions planned for 2027 (pre-review), 2028, 2029, and 2030 (post-review). The 2030 edition will provide a comprehensive assessment of the Compact's implementation against its 2030 horizon, and will inform the post-2030 framework that will succeed the GDC. The Observatory's commitment is to maintain its independent monitoring function throughout this period, providing rigorous, transparent, and timely assessment of GDC implementation.

The long-term implementation horizon poses several challenges that the Observatory will address in subsequent editions. The first is the expansion of country coverage: the 2025 edition covers 68 countries, the 2026 edition will target 100, and subsequent editions will target coverage of all UN member states with sufficient data availability. The second is the refinement of the indicator architecture: the 2025 edition uses 20 indicators across 5 objectives, and subsequent editions will add indicators as new data sources become available and as the Compact's own implementation machinery matures. The third is the development of longitudinal analysis: the 2025 edition is the baseline, and subsequent editions will track changes over time, identifying progress, stagnation, and regression at the country, regional, and global levels. The fourth is the integration of emerging technology horizon-scanning: subsequent editions will include dedicated chapters on quantum computing, neurotechnology, biotechnology, and robotics, as these technologies mature and pose new governance challenges.

13.5 The Observatory's Long-Term Vision

The Observatory's long-term vision is to be the world's leading independent monitoring instrument for the Global Digital Compact and for the broader framework of digital cooperation that will succeed it. The vision is grounded in three commitments. The first is methodological rigour: the Observatory will maintain the highest standards of quantitative measurement, transparent methodology, and reproducible computation. The second is analytical depth: the Observatory will provide not only measurement but also analysis, identifying the drivers, barriers, and forward-looking risks that shape GDC implementation. The third is policy relevance: the Observatory will translate its measurement and analysis into actionable recommendations for governments, international organisations, the private sector, civil society, and the technical community.

The Observatory's long-term vision is also grounded in three partnerships. The first is partnership with the assessed countries: the Observatory will engage with national digital strategy units, data-protection authorities, cybersecurity agencies, and AI governance bodies to ensure that its assessment is accurate, fair, and useful. The

second is partnership with the broader research community: the Observatory will collaborate with universities, think tanks, and other research institutions to ensure that its methodology is at the frontier of digital governance measurement. The third is partnership with the multi-stakeholder community: the Observatory will engage with civil society, the private sector, and the technical community to ensure that its assessment reflects the full range of perspectives on digital governance. The Observatory's success will be measured not by the influence of any single edition but by the cumulative contribution of the annual editions to the Compact's implementation through 2030 and beyond.

13.6 Conclusion

The Observatory's inaugural verdict is one of conditional optimism tempered by structural concern. The Compact is not failing — the global implementation score of 69.2 and the broadly positive trajectory, with 61 of 68 assessed countries on an Improving trajectory, indicate measurable early progress. But the Compact is not succeeding at the pace its 2030 horizon requires. The high-income to low-income gap of 35.7 points is the single most consequential finding. The AI governance objective scores 56.4, the lowest of the five objectives, and the international institutional architecture the Compact mandates is not yet fully operational. The cross-border data-flow fragmentation is widening. The cyber-resilience gap is growing. The AI capability divide is not narrowing.

These findings are not a counsel of despair. They are a diagnosis of the work that remains. The Compact provides the framework; the Observatory provides the measurement; the recommendations in Chapter 12 provide the operational sequence. The road to 2027 begins with this inaugural edition. The road from 2027 to 2030 begins with the high-level review. The road from 2030 to the post-2030 framework begins with the implementation work that this report documents, assesses, and seeks to inform. The Observatory's commitment is to walk these roads with the international community, providing rigorous measurement, transparent methodology, and principled advocacy, for as long as the work of building a just, inclusive, and rights-respecting digital world continues. The work will continue for longer than any single edition, any single institution, or any single generation. The Observatory's institutional commitment is to sustain the measurement of that work, in this inaugural edition and in the editions to come, through 2030 and beyond.

13.7 The Stakes of the 2027 Review

The stakes of the 2027 high-level review are substantial. The review will determine whether the Compact's implementation is on track to meet its 2030 horizon, whether the international institutional architecture is adequate to support implementation, and whether the political will exists to sustain the implementation effort through the end of the decade. The review will also determine the framework for the post-2030 period: whether the Compact is renewed, revised, or replaced, and what the successor framework looks like. The Observatory's view is that the 2027 review should be approached with both ambition and realism: ambition, because the Compact's 2030 horizon requires accelerated implementation; realism, because the implementation gaps documented in this report cannot be closed within the 2025-2027 window alone.

The Observatory's recommendation is that the 2027 review should produce three deliverables. The first is a political declaration reaffirming the Compact's commitments and acknowledging the implementation gaps. The second is an implementation acceleration plan, identifying the specific interventions needed to close the implementation gaps by 2030. The third is a framework for the post-2030 period, establishing the successor to the Compact and the institutional architecture for the next decade of digital cooperation. The Observatory's commitment is to provide rigorous, transparent, and timely analysis to inform each of these deliverables, through the 2025, 2026, and 2027 editions of this report and through the dedicated pre-review edition in mid-2027.

13.8 The Compact's Place in History

The Global Digital Compact's place in history will be determined by its implementation, not by its adoption. The adoption of the Compact on 22 September 2024 was a diplomatic achievement, but it was only the beginning. The Compact's historical significance will depend on whether its commitments translate into measurable improvements in the lives of the 2.2 billion people who remain offline, the many billions more whose interaction with the digital world is mediated by systems they did not design and cannot fully scrutinise, and the communities and ecosystems that are most exposed to the risks of digital technologies, including AI. The Compact's historical significance will also depend on whether its international institutional architecture — ODET, the Scientific Panel, the Global Dialogue — proves adequate to the governance challenges of the 2025-2030 period and beyond.

The Observatory's role is to contribute to the historical record of the Compact's implementation, through rigorous measurement, transparent methodology, and principled advocacy. The inaugural edition of this report is the baseline; each subsequent edition will measure against it, generating a longitudinal record of progress, stagnation, and regression. The Observatory's commitment is to maintain this record through 2030 and beyond, providing the international community with the independent monitoring it needs to assess the Compact's implementation and to design the framework that will succeed it. The road to 2027 begins with this inaugural edition. The road from 2027 to 2030 begins with the high-level review. The road from 2030 to the post-2030 framework begins with the implementation work that this report documents, assesses, and seeks to inform.

Counterarguments and Limitations

Methodological Critique

A rigorous assessment of GDC implementation must engage with the arguments of those who question the Compact's value, its design, or its prospects. The most fundamental critique, advanced by a coalition of over thirty civil society organisations in a joint statement coordinated by Global Partners Digital, is that the GDC is non-binding and therefore lacks the enforcement mechanism needed to translate its commitments into action. On this view, the Compact is a normative statement of aspiration rather than an operational instrument of governance. The critique has merit: the GDC does not include enforcement mechanisms, and its commitments are framed as aspirations rather than obligations. But the critique also understates the value of normative frameworks in shaping state behaviour over time.

A second critique, advanced by scholars of the Global South digital economy, is that the GDC exhibits a techno-solutionist bias that fails to acknowledge the structural inequalities of the global digital economy. On this view, the Compact's emphasis on connectivity, digital skills, and digital public infrastructure treats the symptoms of digital exclusion without addressing their structural causes — the concentration of market power in a small number of platforms, the extractive dynamics of data colonialism, and the asymmetric distribution of compute, talent, and infrastructure.

Limitations of This Index

The Observatory's findings should be interpreted with explicit awareness of four limitations. First, the index is constructed from secondary data and is subject to the coverage, timeliness, and methodological choices of its underlying sources. Second, several indicators rely on proxies where direct measurement is unavailable. Third, the trajectory and forward-looking components are inherently less certain than the retrospective implementation assessment. Fourth, the country sample of 68 countries is biased toward countries with better data availability.

Alternative Frameworks and Their Merits

The Observatory's framework is not the only possible framework for assessing GDC implementation. Several alternative frameworks exist, each with its own merits. The first alternative is the ITU's Global Cybersecurity Index, which provides a single-objective assessment of cybersecurity capacity. The GCI is methodologically mature, broadly accepted, and regularly updated. Its limitation is that it covers only one of the Compact's five objectives. The second alternative is the UN E-Government Development Index, which provides a partial assessment of the inclusive digital economy objective through its measurement of e-government maturity. The EGDI is methodologically mature, broadly accepted, and regularly updated. Its limitation is that it covers only a subset of one of the Compact's five objectives.

The third alternative is the Oxford Insights AI Readiness Index, which provides a single-objective assessment of AI readiness. The AI Readiness Index is methodologically sophisticated and widely cited. Its limitation is that it covers only one of the Compact's five objectives, and that its focus on readiness rather than implementation produces a different analytical perspective. The fourth alternative is the Portulans Network Readiness Index, which provides a composite assessment of digital readiness across multiple dimensions. The NRI is methodologically comprehensive and regularly updated. Its limitation is that its dimensions do not map cleanly onto the Compact's five objectives, and that its focus on readiness rather than implementation produces a different analytical perspective. The Observatory's framework complements these alternatives by providing a comprehensive, multi-objective, implementation-focused assessment that is specifically designed to measure progress against the Compact's commitments.

The Observatory's framework is also distinguishable from the official UN review process. The official review process, mandated by the Compact and conducted through the General Assembly, is intergovernmental and consensus-based. It produces political declarations and outcome documents that reflect the negotiated positions of member states. The Observatory's framework is independent and evidence-based. It produces analytical findings and recommendations that reflect the rigorous application of a transparent methodology to publicly available data. The two processes are complementary: the official process provides the political legitimacy and the policy mandate, while the Observatory's framework provides the analytical rigour and the independent verification. Neither process can substitute for the other; both are needed for a complete assessment of GDC implementation.

Critique of Proxy Indicators

The Observatory's use of proxy indicators — composite measures that substitute for direct measurement where direct measurement is unavailable — is a legitimate target for methodological critique. The critique has three dimensions. The first is the validity critique: do the proxies actually measure what they purport to measure? The MSME digital integration proxy, for example, uses a composite of the Network Readiness Index and the UN E-Government Development Index, on the theory that MSME digital adoption is correlated with the broader digital environment. The theory is plausible but not tautological: in some countries, the broader digital environment may be well-developed while MSME digital adoption lags, or vice versa. The Observatory's response to the validity critique is to document each proxy's rationale, to test each proxy against available direct measures, and to upgrade proxies as better direct measures become available.

The second is the reliability critique: are the proxies stable over time and across contexts? The data-for-SDGs infrastructure proxy, for example, uses a composite of EGDI and DPI maturity, on the theory that the capacity to use data for sustainable development is correlated with overall digital government maturity and DPI deployment. The theory may hold in some contexts but not in others: in countries with mature digital government but limited data-for-SDGs activity, the proxy may overstate the underlying construct. The Observatory's response to the reliability critique is to conduct sensitivity analysis on each proxy (Specification C in the sensitivity analysis) and to report the variation in country classifications that results from proxy substitution. The third is the transparency critique: are the proxies sufficiently documented and reproducible? The Observatory's response to the transparency critique is the full documentation in the Methodology Annex and the publication of the data and code on the Observatory's website.

Trajectory Classification Limitations

The Three-Axis Profile system's trajectory classification — Improving, Stagnating, Deteriorating — is the most analytically ambitious and the most methodologically uncertain component of the Observatory's framework. The trajectory classification is based on the Forward Readiness and Risk Score, which combines a momentum component (recent policy recency and the gap between capacity and implementation) with a risk component (the seven emerging risk signals). The classification is necessarily a simplification of complex dynamics, and several limitations should be acknowledged.

The first limitation is the recency bias: the momentum component gives weight to recent policy activity, which may overstate the trajectory of countries that have recently enacted digital legislation but have not yet translated that legislation into implementation. The second limitation is the risk penalty severity: the risk component applies penalty weights for each of the seven emerging risk signals, which may understate the trajectory of countries that have made recent progress on some risk signals but not others. The third limitation is the binary classification: the trajectory is classified as Improving, Stagnating, or Deteriorating, which obscures the magnitude of the change. A country with a Forward Score of 75 (marginally Improving) and a country with a Forward Score of 90 (strongly Improving) are both classified as Improving, despite the substantial difference in their forward-looking prospects.

The Observatory's response to these limitations is threefold. First, the trajectory classification is reported alongside the underlying Forward Score, so that readers can assess the magnitude of the change as well as the direction. Second, the trajectory classification is treated as one input to the Three-Axis Profile, alongside the Implementation Score and the Governance Capacity Score, so that no country is classified solely on the basis of its trajectory. Third, the trajectory classification is subject to sensitivity analysis (Specification F in the sensitivity analysis), which tests the stability of the classification under alternative risk penalty magnitudes. The

Observatory's commitment is to refine the trajectory classification in subsequent editions as more longitudinal data becomes available and as the methodological feedback from this inaugural edition is incorporated.

The Normative Critique of Measurement

A rigorous assessment of GDC implementation must engage with the normative critique of measurement itself. The critique, advanced by scholars of science and technology studies and by critical data studies, holds that measurement is not a neutral technical activity but a normative political act. The choice of what to measure, how to measure it, and how to present the results reflects substantive judgements about what matters, whose perspectives count, and what kinds of interventions are conceivable. On this view, the Observatory's framework — with its emphasis on quantitative indicators, country-level scores, and comparative rankings — reflects a particular worldview that privileges the measurable over the qualitative, the comparable over the contextual, and the policy-relevant over the politically contestable.

The critique has merit. The Observatory's framework does reflect substantive judgements, and these judgements are open to contestation. The Observatory's response to the normative critique is fourfold. First, the framework's judgements are documented transparently, in the Methodology Note and in the Methodology Annex, so that readers can assess the judgements for themselves. Second, the framework incorporates qualitative analysis alongside quantitative measurement, with approximately 40 per cent of the report's analytical content being qualitative explanation rather than quantitative measurement. Third, the framework is open to methodological critique and revision, with a commitment to publish a methodological changelog in each subsequent edition documenting any indicator additions, source updates, or formula revisions. Fourth, the framework is complemented by other assessment approaches — the official UN review process, the academic literature, the civil society reports — that provide different perspectives on GDC implementation. The Observatory's view is that measurement is a necessary but not sufficient input to the assessment of GDC implementation, and that the normative critique is best addressed through transparency, complementarity, and methodological humility.

The Geopolitical Critique of Universal Frameworks

A rigorous assessment of GDC implementation must also engage with the geopolitical critique of universal frameworks. The critique, advanced by scholars of international relations and by Global South digital policy analysts, holds that universal frameworks — including the GDC itself — reflect the perspectives and interests of the most powerful states, and that the implementation of universal frameworks tends to reproduce rather than challenge existing power asymmetries. On this view, the Compact's emphasis on connectivity, digital skills, digital public infrastructure, and AI governance treats the symptoms of digital exclusion without addressing the structural causes — the concentration of market power, the extractive dynamics of data colonialism, and the asymmetric distribution of compute, talent, and infrastructure.

The critique has merit. The Compact is a negotiated instrument, and the negotiation reflected the relative power of the negotiating parties. The implementation of the Compact will reflect the relative power of the implementing actors. The Observatory's framework, by measuring implementation against the Compact's commitments, may inadvertently reinforce the existing power asymmetries by treating the Compact's framework as the appropriate standard for assessment. The Observatory's response to the geopolitical critique is threefold. First, the framework includes explicit attention to the structural dimensions of digital governance — the AI capability divide, the data colonialism concern, the digital trade fragmentation — that the geopolitical critique highlights. Second, the framework's recommendations include explicit attention to the structural interventions — the Global Fund for AI, the AI governance-capacity divide, the data justice agenda — that the geopolitical critique demands. Third, the framework is open to the inclusion of additional indicators and analytical dimensions that the geopolitical critique may suggest, and the Observatory commits to engaging substantively with any such suggestions in subsequent editions.

Glossary of Key Terms

This glossary defines the key terms used in this report. The definitions are intended to be precise but accessible, and to reflect the usage of the terms in the context of the Global Digital Compact and the Observatory's measurement framework.

At Risk. A Three-Axis Profile classification for countries that face significant forward-looking implementation risk, either because their trajectory is Deteriorating, their trajectory is Stagnating with Implementation below 45, or they are in the transitional zone (Improving, Implementation 73.5 to 77, Capacity below 80).

Capacity Deficit. A diagnostic pattern in which a country's implementation score exceeds its governance capacity score, suggesting that implementation is being sustained by extraordinary effort, leadership, or external support, and is at risk of stalling if capacity is not built.

Capacity Surplus. A diagnostic pattern in which a country's governance capacity score exceeds its implementation score, suggesting that the institutional machinery exists but implementation is lagging due to policy prioritisation, political will, or implementation efficiency constraints.

CBDF. Cross-Border Data Flow. The transfer of data across national borders, subject to regulatory regimes that vary by jurisdiction.

CSTD. Commission on Science and Technology for Development. A UN body that addresses science, technology, and development issues, including the working group on data governance mandated by the GDC.

DPI. Digital Public Infrastructure. The shared digital infrastructure — identity, payments, data exchange — that enables the delivery of public and private digital services.

EGDI. E-Government Development Index. A composite index published by the UN Department of Economic and Social Affairs that measures the readiness and capacity of national e-government.

Forward Readiness and Risk Score. The Observatory's third measurement layer, combining an implementation-momentum component with an emerging-risk-signals component to produce a forward-looking assessment.

Fragile Progress. A Three-Axis Profile classification for countries with implementation scores of at least 45 and an Improving trajectory, but with capacity or forward-looking risks that make the progress fragile.

GCI. Global Cybersecurity Index. An index published by the ITU that measures national cybersecurity capacity, using a tiered system (T1 to T5).

GDC. Global Digital Compact. The UN framework for digital cooperation and AI governance, adopted as UN General Assembly resolution A/RES/79/1 on 22 September 2024.

GDPR. General Data Protection Regulation. The EU's comprehensive data-protection regulation, which entered into force in 2018 and has influenced data-protection legislation globally.

Governance Capacity Score. The Observatory's second measurement layer, aggregating six capacity dimensions to assess whether the institutional machinery exists to carry implementation forward.

Implementer. A Three-Axis Profile classification for countries with an implementation score of at least 56 and an Improving trajectory, subject to the hierarchical decision rules set out in the Methodology Note and Annex B.

Implementation Score. The Observatory's first measurement layer, aggregating twenty indicators across the five GDC objectives, with each objective carrying equal weight (20 per cent).

Leader. A Three-Axis Profile classification for countries with implementation scores of at least 75, capacity scores of at least 70, and an Improving trajectory.

MSME. Micro, Small and Medium-sized Enterprises. The segment of the business population most affected by the digitalisation gap.

ODET. Office for Digital and Emerging Technologies. The UN office established on 1 January 2025 to coordinate the UN system's work on digital cooperation and emerging technologies, succeeding the Office of the Secretary-General's Envoy on Technology.

Score Band. A classification system based on the Implementation Score alone, with five bands: Leader (80+), Implementer (65-80), Fragile Progress (50-65), Stagnating (40-50), At Risk (below 40).

Stagnating. A Three-Axis Profile classification for countries with a Stagnating trajectory, indicating that implementation is neither improving nor deteriorating.

Three-Axis Profile. A classification system based on the interaction of Implementation, Capacity, and Trajectory, producing five profiles: Leader, Implementer, Fragile Progress, Stagnating, At Risk.

Trajectory. The forward-looking direction of a country's implementation, classified as Improving, Stagnating, or Deteriorating based on the Forward Readiness and Risk Score.

WSIS. World Summit on the Information Society. The UN process established in 2003-2005 to address the information society, whose twenty-year review (WSIS+20) is scheduled for 16-17 December 2025.

WSIS+20. The twenty-year review of the World Summit on the Information Society, scheduled for 16-17 December 2025 in New York.

Glossary: Supplementary Terms

The following supplementary terms are used in this report and may be helpful to the reader.

50-in-5. An initiative launched at the GDC's adoption in September 2024, committing countries to design and deliver inclusive, safe, and secure digital public infrastructure by 2028.

AI Safety Institute. A national institution dedicated to AI safety research and pre-deployment evaluation of frontier AI models. The first AI Safety Institute was established in the United Kingdom in November 2023.

Budapest Convention. The Convention on Cybercrime, adopted by the Council of Europe in 2001, which provides a framework for international cooperation on cybercrime investigation and prosecution.

DEPA. Digital Economy Partnership Agreement. A regional trade agreement among Chile, New Zealand, and Singapore, with digital trade provisions.

Frontier AI. AI systems at the frontier of capability, particularly large language models and multimodal foundation models, which pose distinctive risks requiring distinctive governance responses.

Meaningful Connectivity. A framework developed by the Alliance for Affordable Internet that defines meaningful connectivity using four thresholds: a smartphone or larger device, a 4G or higher connection, daily use, and a sufficient speed for productive use.

Malabo Convention. The African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014 and entered into force in 2023.

ODET. Office for Digital and Emerging Technologies. The UN office established on 1 January 2025, succeeding the Office of the Secretary-General's Envoy on Technology.

Pact for the Future. The UN General Assembly resolution adopted at the Summit of the Future on 22 September 2024, to which the Global Digital Compact is annexed.

Resolution 79/325. The UN General Assembly resolution adopted on 26 August 2025, establishing the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on AI Governance.

Scientific Panel. The Independent International Scientific Panel on Artificial Intelligence, established by General Assembly resolution 79/325. The 40 members are expected to be appointed in early 2026.

Summit of the Future. The UN high-level summit held in New York on 22-23 September 2024, at which the Pact for the Future and the Global Digital Compact were adopted.

Usage Gap. The gap between mobile broadband coverage and actual usage, affecting an estimated 3.4 billion people who live in areas covered by mobile broadband but do not use it.

WSIS Action Lines. The action lines established by the World Summit on the Information Society to implement the WSIS outcomes, covering the range of digital cooperation issues.

Annex A — GDC Governance Index 2025: Country Rankings

The following table presents the full ranking of the 68 assessed countries, ordered by GDC Implementation Score. The table reports both classification systems.

Annex B — Methodology Annex

B.1 Indicator Dictionary

B.2 Sensitivity Analysis

The Observatory tested classification stability under six alternative specifications: (A) baseline; (B) objective weight plus or minus 10 per cent; (C) proxy removal; (D) alternative GCI mapping; (E) population-weighted; (F) risk penalty halving. 47 of 68 countries (69 per cent) maintain the same Three-Axis Profile across all specifications.

Annex C — References

[1] African Union (2024). Continental Artificial Intelligence Strategy. https://au.int

[2] Advocacy Unified Network (2024). Governing the Digital Frontier. The Hague: AUN.

[3] Advocacy Unified Network (2025). From Readiness to Implementation. The Hague: AUN.

[4] European Commission (2025). Adequacy Decisions. https://commission.europa.eu

[5] International Telecommunication Union (2025). Facts and Figures 2025. Published 17 November 2025.

[6] International Telecommunication Union (2024). Global Cybersecurity Index 2024.

[7] Stanford HAI (2025). Artificial Intelligence Index Report 2025.

[8] United Nations (2024). Global Digital Compact (A/RES/79/1).

[9] United Nations (2025). Resolution 79/325: Artificial Intelligence.

[10] UN DESA (2024). UN E-Government Survey 2024.

[11] UNCTAD (2025). Technology and Innovation Report 2025.

[12] World Economic Forum (2025). Future of Jobs Report 2025.

[13] World Economic Forum (2025). Global Risks Report 2025.

Annex D — Selected Country Profiles

Each profile heading shows the country's Three-Axis Profile classification, generated directly from the Annex A dataset.

Singapore — Leader

Implementation: 87.5 | Capacity: 90.1 | Forward: 70.4 | Trajectory: Improving | Score Band: Leader | Profile: Leader

Objective Scores — Divides: 94.2; Economy: 94.9; Safety: 92.3; Data: 79.2; AI: 76.9.

Estonia — Leader

Implementation: 86.9 | Capacity: 89.5 | Forward: 70.4 | Trajectory: Improving | Score Band: Leader | Profile: Leader

Objective Scores — Divides: 88.2; Economy: 92.6; Safety: 94.5; Data: 87.6; AI: 71.5.

United Arab Emirates — Leader

Implementation: 86.2 | Capacity: 86.0 | Forward: 74.9 | Trajectory: Improving | Score Band: Leader | Profile: Leader

Objective Scores — Divides: 87.2; Economy: 84.5; Safety: 94.9; Data: 85.3; AI: 79.0.

India — At Risk

Implementation: 74.0 | Capacity: 74.0 | Forward: 67.8 | Trajectory: Improving | Score Band: Implementer | Profile: At Risk

Objective Scores — Divides: 67.7; Economy: 71.9; Safety: 93.9; Data: 73.6; AI: 63.1.

Brazil — At Risk

Implementation: 76.4 | Capacity: 78.6 | Forward: 72.4 | Trajectory: Improving | Score Band: Implementer | Profile: At Risk

Objective Scores — Divides: 73.4; Economy: 73.6; Safety: 92.2; Data: 79.7; AI: 63.3.

Rwanda — Implementer

Implementation: 62.0 | Capacity: 65.6 | Forward: 69.0 | Trajectory: Improving | Score Band: Fragile Progress | Profile: Implementer

Objective Scores — Divides: 35.9; Economy: 49.7; Safety: 87.5; Data: 75.7; AI: 61.4.

Kenya — Implementer

Implementation: 64.3 | Capacity: 68.6 | Forward: 70.3 | Trajectory: Improving | Score Band: Fragile Progress | Profile: Implementer

Objective Scores — Divides: 40.7; Economy: 54.7; Safety: 89.2; Data: 73.7; AI: 63.2.

South Africa — Implementer

Implementation: 66.7 | Capacity: 66.6 | Forward: 68.9 | Trajectory: Improving | Score Band: Implementer | Profile: Implementer

Objective Scores — Divides: 61.8; Economy: 67.1; Safety: 84.2; Data: 54.4; AI: 65.8.

China — Leader

Implementation: 79.5 | Capacity: 81.0 | Forward: 66.2 | Trajectory: Improving | Score Band: Implementer | Profile: Leader

Objective Scores — Divides: 75.2; Economy: 82.8; Safety: 95.7; Data: 73.1; AI: 70.6.

United States — At Risk

Implementation: 75.4 | Capacity: 83.2 | Forward: 37.6 | Trajectory: Deteriorating | Score Band: Implementer | Profile: At Risk

Objective Scores — Divides: 86.9; Economy: 90.1; Safety: 86.5; Data: 61.6; AI: 51.9.

Germany — Leader

Implementation: 84.7 | Capacity: 87.4 | Forward: 69.3 | Trajectory: Improving | Score Band: Leader | Profile: Leader

Objective Scores — Divides: 85.2; Economy: 86.1; Safety: 94.4; Data: 86.5; AI: 71.3.

Myanmar — At Risk

Implementation: 34.0 | Capacity: 28.7 | Forward: 44.8 | Trajectory: Stagnating | Score Band: At Risk | Profile: At Risk

Objective Scores — Divides: 22.1; Economy: 26.7; Safety: 52.4; Data: 54.6; AI: 13.9.

Annex E — GDC Commitment Implementation Tracker

About the Advocacy Unified Network

Advocacy Unified Network (AUN) is a global public policy research and advocacy organisation headquartered in The Hague, Netherlands. The AUN Global Digital Compact Observatory, launched with this inaugural report, is the flagship institutional product of the Digital programme. For more information, visit aunetwork.org.

AUN Global Digital Compact Observatory · Inaugural Edition · 1 December 2025

ADVOCACY UNIFIED NETWORK AUN Global Digital Compact Observatory

Published	1 December 2025
Publisher	Advocacy Unified Network (AUN), The Hague

DOI: 10.62692/opus.gdc.2025.12 | Advocacy Unified Network (AUN)

Imprint	Opus Publica — AUN Digital / CyberSec Programme
Document Type	Independent Flagship Research Report
Edition	Inaugural Edition — Baseline for the 2027 High-Level Review

What This Index Does NOT Measure The AUN GDC Governance Index measures national implementation of the GDC's commitments. It does NOT measure: citizen satisfaction with digital public services; quality of individual AI systems; national GDP impact of digitalisation; internet freedom as a standalone construct; cybersecurity incident frequency; actual enforcement effectiveness of data-protection laws; environmental footprint of digital technologies; distributional impacts within countries.

Rule	Profile	Condition
1	At Risk	Trajectory is Deteriorating
2	Stagnating	Trajectory is Stagnating AND Implementation at least 45
3	At Risk	Trajectory is Stagnating AND Implementation below 45
4	At Risk	Improving AND Implementation >= 73.5 AND Implementation < 77 AND Capacity < 80 (transitional zone)
5	Leader	Implementation at least 75 AND Capacity at least 70 AND Improving
6	Implementer	Implementation at least 56 AND Improving
7	Fragile Progress	Implementation at least 45 AND Improving
8	At Risk	Fallback (no other rule matched)

Case Study — India: DPI at Scale (Score: 74.0/100) India's Digital Public Infrastructure represents one of the most comprehensive operationalisations of the GDC's DPI commitments. The Aadhaar digital identity system has enrolled over 1.3 billion residents; the Unified Payments Interface processes more than 10 billion transactions per month; and the DigiLocker data-exchange layer hosts more than 6 billion documents. India's GDC Implementation Score is 74.0, with an Objective 1 score of 67.7. Digital public infrastructure, including Aadhaar (launched 2009) and UPI (launched 2016), has contributed to improvements in financial inclusion and service delivery efficiency.

Case Study — Rwanda: Targeted Investment in a Low-Income Context (Score: 62.0/100) Rwanda demonstrates that targeted investment can produce disproportionate returns even in resource-constrained environments. With a GNI per capita of approximately $930, Rwanda has achieved Tier 1 status in the ITU Global Cybersecurity Index, established a national digital identity system (NIDA), deployed the Irembo e-government platform covering over 100 public services, and adopted a national AI policy in 2023. Rwanda's GDC Implementation Score is 62.0. Internet penetration remains at 30.0 per cent, and mobile broadband affordability at 8.7 per cent of monthly GNI per capita is well above the 2 per cent target.

Case Study — Brazil: Pix and the Digital Payments Revolution (Score: 76.4/100) Brazil's Pix instant payment system, launched by the Central Bank of Brazil in November 2020, has transformed the country's digital economy. As of late 2025, Pix has over 160 million registered users and processes over 4 billion transactions per month. Brazil's GDC Implementation Score is 76.4, with an Objective 2 score of 73.6.

Case Study — Estonia: The Pioneer of Digital State Resilience (Score: 86.9/100) Estonia, with a population of 1.3 million and an EGDI score of 0.9727 (third globally), has established itself as a global reference point for digital state resilience. The Estonian digital infrastructure is anchored in the e-ID digital identity system, the X-Road data-exchange layer, and the KSI blockchain integrity system. Estonia's GDC Implementation Score is 86.9, with an Objective 3 score of 94.5.

Case Study — Ghana: Building Cybersecurity Capacity in a Middle-Income Context (Score: 63.3/100) Ghana, with a GNI per capita of approximately $2,500, has achieved Tier 1 status in the ITU Global Cybersecurity Index, demonstrating that targeted investment in cybersecurity capacity can produce disproportionate returns even in resource-constrained environments. Ghana's GDC Implementation Score is 63.3, with an Objective 3 score of 84.5.

Case Study — United Arab Emirates: Regional Digital Leadership (Score: 86.2/100) The United Arab Emirates has positioned itself as a regional leader in digital governance, anchored in its Federal Personal Data Protection Law (2021, revised 2022), its AI Strategy 2031, and its UAE Pass digital identity system. The UAE's GDC Implementation Score is 86.2. The UAE has not received an EU GDPR adequacy decision.

Case Study — India: DPDP Act and Cross-Border Data Flow (Score: 74.0/100) India's Digital Personal Data Protection Act 2023 represents a distinctive approach that combines comprehensive data-protection standards with significant cross-border data-transfer restrictions. India's GDC Implementation Score on Objective 4 is 73.6.

Case Study — United States: Investment Leadership, Regulatory Volatility (Score: 75.4/100) The United States accounts for approximately 70 per cent of global private AI investment. President Biden's Executive Order on AI (October 2023) was revoked by President Trump in January 2025 and replaced by an AI Action Plan. The US GDC Implementation Score is 75.4, with a Three-Axis Profile of At Risk due to its deteriorating trajectory (Forward Readiness Score: 37.6). The absence of a comprehensive federal data-protection law remains the single most consequential implementation gap.

Case Study — China: State-Led AI Development (Score: 79.5/100) China is the world's second-largest AI investment market. China's GDC Implementation Score is 79.5, with a Three-Axis Profile of Leader. The cross-border data-flow regime is restrictive.

Case Study — Kenya: Digital Finance and the Silicon Savannah (Score: 64.3/100) Kenya has positioned itself as East Africa's digital hub, anchored in the M-Pesa mobile money platform (launched 2007, now serving over 30 million users), the Konza Technopolis project, and a robust ecosystem of fintech, agritech, and healthtech startups. Kenya's GDC Implementation Score is 64.3, with an Objective 1 score of 40.7 and an Objective 2 score of 54.7. Internet penetration stands at 42.0 per cent. The Kenyan case illustrates the potential of digital finance to drive financial inclusion and economic activity in lower-middle-income contexts, while also highlighting the persistence of rural-urban divides, the gender gap in mobile money adoption, and the need for sustained investment in digital skills and infrastructure.

Case Study — Ghana: Cybersecurity Leadership in a Middle-Income Context (Score: 63.3/100) Ghana has positioned itself as a cybersecurity leader in West Africa, anchored in the Cybersecurity Act 2020, the National Cybersecurity Centre, and the Computer Emergency Response Team (CERT). Ghana has achieved Tier 1 status in the ITU Global Cybersecurity Index, demonstrating that targeted investment in cybersecurity capacity can produce disproportionate returns even in resource-constrained environments. Ghana's GDC Implementation Score is 63.3, with an Objective 3 score of 84.5. The Ghanaian case illustrates the potential for middle-income countries to leapfrog in specific dimensions of digital governance, while also highlighting the persistence of broader implementation gaps in connectivity, digital skills, and AI governance.

Case Study — South Korea: Cybersecurity Maturity in a High-Threat Environment (Score: 84.4/100) South Korea has developed one of the world's most mature cybersecurity postures, driven by the persistent threat environment on the Korean peninsula. The National Intelligence Service's Cyber Security Center, the Korea Internet and Security Agency (KISA), and the Ministry of Science and ICT's cybersecurity division form a robust institutional architecture. South Korea's GDC Implementation Score is 84.4, with an Objective 3 score of 91.6. The Korean case illustrates how sustained investment in cybersecurity capacity, driven by an acute threat environment, can produce world-class capability — but also how the broader digital safety agenda (information integrity, child online protection) requires continued attention alongside the core cybersecurity mission.

Case Study — Rwanda: Cybersecurity Leadership in a Low-Income Context (Score: 62.0/100) Rwanda has positioned itself as a cybersecurity leader in the East African Community, anchored in the National Cyber Security Authority (NCSA), the Rwanda Computer Emergency Response Team (RW-CERT), and a comprehensive legal framework including the Law on Cybercrime (2018). Rwanda has achieved Tier 1 status in the ITU Global Cybersecurity Index, demonstrating that targeted investment in cybersecurity capacity can produce disproportionate returns even in low-income contexts. Rwanda's GDC Implementation Score is 62.0, with an Objective 3 score of 87.5. The Rwandan case illustrates that cybersecurity capacity is not solely a function of income level, and that strategic prioritisation can produce world-class capability in specific dimensions.

Case Study — Japan: AI Strategy in an Ageing Society (Score: 82.6/100) Japan has positioned itself as a leader in human-centric AI governance, driven by the unique demographic context of a rapidly ageing society and the corresponding need to deploy AI to augment a shrinking workforce. The Integrated Innovation Strategy Promotion Council, the AI Strategy Council, and the Social Principles of Human-centric AI provide the institutional and normative framework. Japan's GDC Implementation Score is 82.6, with an Objective 5 score of 69.2. The Japanese case illustrates how demographic context shapes AI strategy, and how the human-centric framing can be operationalised through specific institutional and normative commitments.

Case Study — South Korea: AI National Strategy and the Digital New Deal (Score: 84.4/100) South Korea has positioned itself as a global AI leader through the National Strategy for Artificial Intelligence (2019), the Digital New Deal (2020), and the AI Basic Act (2024). The Korean approach combines substantial public investment in AI infrastructure and research, a robust regulatory framework, and active support for AI adoption in industry. South Korea's GDC Implementation Score is 84.4, with an Objective 5 score of 73.8. The Korean case illustrates the potential of a comprehensive national AI strategy, combining investment, regulation, and adoption support, to produce measurable AI capability.

Case Study — African Union: Continental AI Strategy (Score: derived from AU member state assessments) The African Union's Continental Artificial Intelligence Strategy, endorsed by the Executive Council in July 2024, is the first regional AI strategy covering 55 member states. The Strategy commits AU members to develop national AI strategies, invest in AI infrastructure and skills, and participate in international AI governance dialogue. The Strategy is significant because it provides a regional framework for AI governance in a continent where individual national AI strategies are still emerging. The implementation of the Strategy will be tracked in subsequent editions of this report through the assessment of AU member states' AI governance indicators. Of the African countries assessed in this inaugural edition, South Africa (65.8), Kenya (63.2), Rwanda (61.4), Ghana (58.7), and Egypt (30.7) provide early indications of the continental trajectory.

#	Recommendation	Action
1	Operationalise AI Scientific Panel and Global Dialogue	Complete appointment of 40 Panel members; hold first Global Dialogue in July 2026
2	Establish the Global Fund for AI	Initial capitalisation of $1 billion by end 2026; trajectory to $3 billion by 2028
3	Develop a global DPI safeguards framework	Convene multi-stakeholder process by end 2026
4	Address the AI governance-capacity divide	Prioritise AI capacity-building; allocate 60% of Fund to Global South
5	Align national digital strategies with the GDC	Develop mapping toolkit by March 2026
6	Accelerate CSTD working group on data governance	Prioritise cross-border data-flow interoperability
7	Strengthen the Internet Governance Forum	Align 2026-2027 IGF programmes with GDC objectives
8	Develop GDC implementation monitoring framework	Draw on independent monitoring initiatives
9	Address digital rights and civic space deficit	Develop human rights due diligence framework
10	Establish emerging technology horizon-scanning	Annual report on quantum, neurotech, biotech, robotics

Rank	Country	Region	Income	Impl.	Cap.	Fwd.	Traj.	Score Band	3-Axis Profile
1	Sweden	Europe	HIC	87.6	89.4	69.0	Impro	Leader	Leader
2	Singapore	Southeast Asia	HIC	87.5	90.1	70.4	Impro	Leader	Leader
3	Netherlands	Europe	HIC	87.2	88.8	70.1	Impro	Leader	Leader

4	United Kingdom	Europe	HIC	87.1	89.1	72.3	Impro	Leader	Leader
5	Norway	Europe	HIC	87.0	88.5	71.1	Impro	Leader	Leader
6	Estonia	Europe	HIC	86.9	89.5	70.4	Impro	Leader	Leader
7	United Arab Emirates	MENA	HIC	86.2	86.0	74.9	Impro	Leader	Leader
8	Australia	Oceania	HIC	85.7	88.2	70.3	Impro	Leader	Leader
9	New Zealand	Oceania	HIC	85.1	86.4	71.0	Impro	Leader	Leader
10	Germany	Europe	HIC	84.7	87.4	69.3	Impro	Leader	Leader
11	South Korea	East Asia	HIC	84.4	87.6	70.6	Impro	Leader	Leader
12	Spain	Europe	HIC	84.4	86.2	72.3	Impro	Leader	Leader
13	France	Europe	HIC	84.3	86.9	69.3	Impro	Leader	Leader
14	Japan	East Asia	HIC	82.6	82.0	72.8	Impro	Leader	Leader
15	Portugal	Europe	HIC	80.7	83.3	70.4	Impro	Leader	Leader
16	Italy	Europe	HIC	79.7	79.8	72.8	Impro	Implementer	Leader
17	Saudi Arabia	MENA	HIC	79.6	77.6	65.7	Impro	Implementer	Leader
18	China	East Asia	UMIC	79.5	81.0	66.2	Impro	Implementer	Leader
19	Qatar	MENA	HIC	77.9	78.4	69.7	Impro	Implementer	Leader
20	Poland	Europe	HIC	77.4	78.3	74.1	Impro	Implementer	Leader
21	Israel	MENA	HIC	77.0	78.1	71.0	Impro	Implementer	Leader
22	Canada	N.Am.	HIC	76.8	84.2	69.8	Impro	Implementer	Leader
23	Brazil	LAC	UMIC	76.4	78.6	72.4	Impro	Implementer	At Risk
24	United States	N.Am.	HIC	75.4	83.2	37.6	Deter	Implementer	At Risk
25	Greece	Europe	HIC	74.7	75.2	75.1	Impro	Implementer	At Risk
26	Chile	LAC	HIC	74.1	74.6	71.8	Impro	Implementer	At Risk
27	India	South Asia	LMIC	74.0	74.0	67.8	Impro	Implementer	At Risk
28	Malaysia	Southeast Asia	UMIC	74.0	76.3	72.4	Impro	Implementer	At Risk
29	Thailand	Southeast Asia	UMIC	73.9	73.4	72.8	Impro	Implementer	At Risk
30	Jordan	MENA	LMIC	73.2	71.4	74.9	Impro	Implementer	Implementer
31	Russia	CIS	UMIC	71.2	68.6	65.7	Impro	Implementer	Implementer
32	Kazakhstan	Central Asia	UMIC	70.4	67.3	67.8	Impro	Implementer	Implementer
33	Uruguay	LAC	HIC	69.9	71.7	71.2	Impro	Implementer	Implementer
34	Colombia	LAC	UMIC	69.8	70.2	72.9	Impro	Implementer	Implementer
35	Armenia	CIS	UMIC	69.4	68.4	73.8	Impro	Implementer	Implementer
36	Costa Rica	LAC	HIC	69.2	71.5	70.3	Impro	Implementer	Implementer
37	Vietnam	Southeast Asia	LMIC	68.6	66.8	67.8	Impro	Implementer	Implementer
38	Georgia	CIS	UMIC	67.0	69.1	73.5	Impro	Implementer	Implementer
39	South Africa	SSA	UMIC	66.7	66.6	68.9	Impro	Implementer	Implementer
40	Indonesia	Southeast Asia	UMIC	66.6	66.4	66.8	Impro	Implementer	Implementer

41	Sri Lanka	South Asia	LMIC	65.9	66.5	75.1	Impro	Implementer	Implementer
42	Mexico	LAC	UMIC	65.0	68.2	69.5	Impro	Implementer	Implementer
43	Ukraine	CIS	LMIC	64.8	65.9	70.9	Impro	Fragile Progress	Implementer
44	Kenya	SSA	LMIC	64.3	68.6	70.3	Impro	Fragile Progress	Implementer
45	Uzbekistan	Central Asia	LMIC	64.1	59.1	67.8	Impro	Fragile Progress	Implementer
46	Morocco	MENA	LMIC	63.8	67.0	76.0	Impro	Fragile Progress	Implementer
47	Philippines	Southeast Asia	LMIC	63.7	65.7	72.4	Impro	Fragile Progress	Implementer
48	Ghana	SSA	LMIC	63.3	65.5	74.6	Impro	Fragile Progress	Implementer
49	Argentina	LAC	UMIC	63.1	67.7	71.0	Impro	Fragile Progress	Implementer
50	Mongolia	East Asia	LMIC	62.2	62.4	66.8	Impro	Fragile Progress	Implementer
51	Rwanda	SSA	LIC	62.0	65.6	69.0	Impro	Fragile Progress	Implementer
52	Peru	LAC	UMIC	62.0	62.5	71.9	Impro	Fragile Progress	Implementer
53	Bangladesh	South Asia	LMIC	61.5	60.8	74.9	Impro	Fragile Progress	Implementer
54	Jamaica	LAC	UMIC	60.8	57.8	68.8	Impro	Fragile Progress	Implementer
55	Egypt	MENA	LMIC	60.6	60.7	58.7	Impro	Fragile Progress	Implementer
56	Belarus	CIS	UMIC	59.7	56.4	59.7	Impro	Fragile Progress	Implementer
57	Nigeria	SSA	LMIC	56.1	57.1	68.1	Impro	Fragile Progress	Implementer
58	Cote dIvoire	SSA	LMIC	55.9	53.6	70.9	Impro	Fragile Progress	Fragile Progress
59	Tanzania	SSA	LMIC	54.6	58.9	63.3	Impro	Fragile Progress	Fragile Progress
60	Tunisia	MENA	LMIC	54.4	59.1	48.9	Deter	Fragile Progress	At Risk
61	Pakistan	South Asia	LMIC	53.0	54.5	62.3	Impro	Fragile Progress	Fragile Progress
62	Nepal	South Asia	LMIC	52.9	53.6	66.2	Impro	Fragile Progress	Fragile Progress
63	Fiji	Oceania	UMIC	52.1	50.3	64.9	Impro	Fragile Progress	Fragile Progress
64	Ethiopia	SSA	LIC	45.2	41.1	52.9	Stagn	Stagnating	Stagnating
65	Senegal	SSA	LMIC	43.1	45.3	48.4	Deter	Stagnating	At Risk

66	Cambodia	Southeast Asia	LMIC	41.5	37.0	51.8	Stagn	Stagnating	At Risk
67	Uganda	SSA	LIC	41.3	42.1	47.8	Stagn	Stagnating	At Risk
68	Myanmar	Southeast Asia	LIC	34.0	28.7	44.8	Stagn	At Risk	At Risk

#	Indicator	Source	Year	Normalisation
1.1	Internet penetration	ITU F&F	2025	Linear 0-100%
1.2	Affordability	ITU F&F	2025	Logarithmic
1.3	Digital skills index	ITU/UNESCO	2024	Direct
1.4	DPI maturity	World Bank	2024	Discrete mapping
2.1	E-government dev.	UN EGDI	2024	Linear x100
2.2	Online service part.	UN EGDI	2024	Direct
2.3	Digital fin. inclusion	AUN proxy	2025	DPI x MBB
2.4	MSME digital integration	AUN proxy	2025	NRI x EGDI
3.1	Cybersecurity capacity	ITU GCI	2024	Midpoint map
3.2	Cybercrime legislation	UNCTAD	2024	Binary
3.3	Child online safety	AUN proxy	2025	GCI x Cyberlaw
3.4	Information integrity	AUN proxy	2025	NRI x DPlaw
4.1	DP legislation	UNCTAD/OECD	2024	Recency scale
4.2	CBDF openness	EU/WTO/ITIF	2025	Discrete mapping
4.3	Data-for-SDGs infra.	AUN proxy	2025	EGDI x DPI
4.4	DG institutions	AUN proxy	2025	DP x Cyber x DPI
5.1	National AI strategy	OECD.AI/HAI	2025	Recency scale
5.2	AI capacity index	Oxford/HAI	2025	Direct
5.3	AI governance inst.	AUN proxy	2025	AI x DP x GCI
5.4	AI skills & research	AUN proxy	2025	AIcap x Skills

#	GDC Commitment	Status	Key Challenge
1.1	Connect remaining offline population by 2030	In Progress	2.2B remain offline (ITU 2025)
1.2	Develop DPI safeguards	Initiated	No global standard agreed
2.1	Foster open digital environment for MSMEs	In Progress	MSME e-commerce 10-15% in LMICs
3.1	Refrain from internet shutdowns	Initiated	196 shutdowns in 2024
4.1	Strengthen national data governance	Substantially Achieved	137 countries have DP law
5.1	Establish Independent Scientific Panel on AI	In Progress	40 members expected early 2026
5.2	Initiate Global Dialogue on AI Governance	In Progress	First convening scheduled July 2026