ESCAP
Economic and Social Commission for Asia and the Pacific

ECA

UNITED NATIONS
ECLAC

Regional Digital Trade Integration Index 2.0: A Guide

ESCAP-ECA-ECLAC Initiative on Digital Trade Regulatory Integration

The United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) is the most inclusive intergovernmental platform in the Asia-Pacific region. The Commission promotes cooperation among its 53 member States and nine associate members in pursuit of solutions to sustainable development challenges. ESCAP is one of the five regional commissions of the United Nations. The ESCAP Secretariat supports inclusive, resilient and sustainable development in the region by generating action-oriented knowledge and by providing technical assistance and capacity-building services in support of national development objectives, regional agreements and the implementation of the 2030 Agenda for Sustainable Development.

The Economic Commission for Africa (ECA) is made up of 54 member States, and plays a dual role as a regional arm of the United Nations and as a key component of the African institutional landscape, and therefore well positioned to make unique contributions to address the Continent's development challenges. The contribution by ECA to the task of carrying forward the United 2030 Agenda and African Union (AU) Agenda 2063 is centred on the Commission's three core functions, namely, its convening function, its function as a think tank and its operational function.

ECA's mission is guided by its five new strategic directions which are: (1) advancing ECA's position as a premier knowledge institution that builds on its unique position and privilege to bring global solutions to the continent's problems and take local solution to the continent; (2) developing macroeconomic and structural policy options to accelerate economic diversification and job creation; (3) designing and implementing innovative financing models for infrastructure, and for human, physical and social assets for transforming Africa; (4) contributing solutions to regional and transboundary challenges, with a focus on peace security and social inclusion as an important development nexus; (5) advocating Africa's position at the global level and developing regional responses as a contribution to global governance issues. As a specialized unit of ECA, the African Trade Policy Centre (ATPC) supports the efforts of member States and regional economic communities by enhancing their capacity to formulate and implement sound trade policies and participate more effectively in trade negotiations at all levels. To this end, the Centre is engaged in policy research, capacity-building, technical assistance and advocacy.

The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) has 46 member States and 14 Associate Members. The overall purpose of ECLAC is to promote the economic, social and environmentally sustainable development of Latin America and the Caribbean through continuous international cooperation, by undertaking comprehensive research and analysis of development processes and providing relevant normative, operational and technical cooperation services in support of regional development efforts. The Commission's mandate derives from Economic and Social Council Resolution 106 (VI), by which the Council established the Commission for the purpose of contributing to and co-ordinating action towards the economic and social development of the region and strengthening the economic relationships among the countries of the region as well as with other countries of the world. In 1996, by virtue of ECLAC Resolution 553(XXVI), the Commission was instructed, inter alia, to collaborate with member States in a comprehensive analysis of development processes geared to the design, monitoring and evaluation of public policies and the resulting provision of operational services in the fields of specialized information, advisory services, training and support for regional and international cooperation and coordination.

For further information on this publication, please contact: escap-tiid@un.org.
ECLAC Symbol: LC/TS.2024/51

Regional Digital Trade Integration Index 2.0: A Guide

July 2024

ESCAP-ECA-ECLAC Initiative on
Digital Trade Regulatory Integration

Disclaimer

The views expressed in this publication are those of the authors and do not necessarily reflect the views of ESCAP. The designations employed and the presentation of the material in this report do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any economy, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The United Nations bears no responsibility for the availability or functionality of URLs.

The opinion, figures and estimates set forth in this publication are the responsibility of the authors and should not necessarily be considered as reflecting the views or carrying the endorsement of the United Nations. Any errors are the responsibility of the authors. Mention of firm names and commercial products does not imply the endorsement of the United Nations.

This report has been issued without formal editing.

Please cite this publication as:

United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), Economic Commission for Africa (ECA) and Economic Commission for Latin America and the Caribbean (ECLAC), 2024. Regional Digital Trade Integration Index 2.0: A Guide. June 2024. Bangkok: ESCAP. Available at https://hdl.handle.net/20.500.12870/6849

Acknowledgements

This publication was prepared by the Trade, Investment, and Innovation Division (TIID) of ESCAP, in collaboration with the United Nations Economic Commission for Africa (ECA), and the Economic Commission for Latin America and the Caribbean (ECLAC).

Under the overall guidance of Rupa Chanda, Director of TIID, and with the substantive guidance and inputs of Yann Duval, Chief of the Trade Policy and Facilitation Section (TPFS), TIID, ESCAP, the preparation of this publication was managed by Witada Anukoonwattaka, Economic Affairs Officer and the RDTII project coordinator at ESCAP. Initially created at ESCAP and based on the technical contributions of Martina F. Ferracane, the RDTII methodology underwent further development through a cooperative effort involving ESCAP, ECA, ECLAC and the European University Institute.

This version of the Guide is intended to accompany RDTII version 2.0. ESCAP is grateful for feedbacks and inputs provided by the ESCAP team (Fandi Achmad, Natnicha Sutthivana, Ziyu Qiao, Alexandre Germouty, Thamolwan Pingmuang and Ivan Cenon Bernardo), ECA (Simon Mevel, Jason Mccormack and Geoffroy Guepie) and ECLAC (Nanno Mulder and Alejandro Fredes). It is an updated document from the first version, released in April 2022.

Preface

This RDTII Guide, now in its second edition, serves as a handbook designed to assist policymakers and policy researchers in analysing digital trade regulations. The Guide complements RDTII version 2.0, a common framework developed in collaboration with the European University Institute and utilized by ESCAP, ECA and ECLAC for digital trade regulatory analysis. Users of this guide are recommended to use it in conjunction with the ESCAP-ECA-ECLAC Digital Trade Regulatory Review for Asia-Pacific, Africa, Latin America and the Caribbean, 2023 and 2024 versions.

The guide provides essential explanations of the structure and rationale of RDTII 2.0, along with guidance on data collection and sources. It is also useful for those who will use the index and related indicators for policy analysis. The RDTII framework, a multidimensional cross-economy index of digital trade regulatory integration, is expected to require continuous adjustments as the challenges and policy trade-offs associated with the fast-growing digital trade and the global digital economy are better understood. As such, this guide is considered a living document to be updated as the United Nations Regional Commissions and partners work together to further improve the index and the data collection process.

Contents

Acknowledgements iii

Preface iv

Abbreviations and acronyms viii

Chapter 1. Conceptual framework 1

Background 2

Lowering regulatory compliance costs and enhancing interoperability as the basis for regional digital trade integration 2

The Regional Digital Trade Integration Index (RDTII) 2.0: Indicating the regulatory costs of doing regional business digitally 3

Chapter 2. RDTII 2.0 framework 6

Scoring methodology 7

Sources of regulatory measures 9

Lack of regulatory measures 9

Chapter 3. RDTII 2.0 pillars 10

Pillar 1. Tariffs and trade defence 11

Pillar 2. Public procurement 15

Pillar 3. Foreign direct investment 21

Pillar 4. Intellectual property rights 26

Pillar 5. Telecommunications regulations and competition 34

Pillar 6. Cross-border data policies 41

Pillar 7. Domestic data protection and privacy 49

Pillar 8. Internet intermediary liability 55

Pillar 9. Content access 60

Pillar 10. Non-technical NTMs 65

Pillar 11. Standards and procedures 69

Pillar 12. Online sales and transactions 75

Chapter 4. Concluding remarks 83

Annexes

Annex I. Step-by-step guide to create data for indicators 1.1 and 1.2 85

Annex II. ITA I, ITA II and ITA III products 91

References 103

List of Boxes

Box 1.	The RDTII 2.0 framework in brief	4
Box 2.	The Agreement on Government Procurement (GPA)	19
Box 3.	The Patent Cooperation Treaty (PCT)	28
Box 4.	The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)	31
Box 5.	WTO Telecom Reference Paper	38
Box 6.	International encryption standards for import encryption methods	73
Box 7.	Relationship among the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures and the United Nations Convention on the Use of Electronic Communications	81

List of Figures

Figure 1. Simplification and interoperability of digital trade rules 2
Figure 2. Regional Digital Trade Regulatory Integration Index (RDTII 2.0) – Pillars and indicators 5
Figure 3. RDTII 2.0 methodology 7
Figure 4. Republic of Korea's regulatory measures 9
Figure 5. Tension among different policy objectives in Pillar 1 11
Figure 6. Pillar 1 indicators and the weights 14
Figure 7. Tension among different policy objectives in Pillar 2 15
Figure 8. Pillar 2 indicators and the weights 20
Figure 9. Tension among different policy objectives in Pillar 3 21
Figure 10. Pillar 3 indicators and the weights 25
Figure 11. Balance in different policy objectives in Pillar 4 26
Figure 12. Pillar 4 indicators and the weights 33
Figure 13. Balance in different policy objectives in Pillar 5 34
Figure 14. Pillar 5 indicators and the weights 40
Figure 15. Balance in different policy objectives in Pillar 6 41
Figure 16. Conditions of consent, evaluation and approval 46
Figure 17. Pillar 6 indicators and the weights 48
Figure 18. Balance in different policy objectives in Pillar 7 49
Figure 19. Pillar 7 indicators and the weights 54
Figure 20. Balance in different policy objectives in Pillar 8 55
Figure 21. Pillar 8 indicators and the weights 59
Figure 22. Balance in different policy objectives in Pillar 9 60
Figure 23. Pillar 9 indicators and the weights 64
Figure 24. Tension among different policy objectives in Pillar 10 65
Figure 25. Pillar 10 indicators and the weights 68
Figure 26. Balance in different policy objectives in Pillar 11 69
Figure 27. Pillar 11 indicators and the weights 74
Figure 28. Balance in different policy objectives in Pillar 12 75
Figure 29. Pillar 12 indicators and the weights 82

Abbreviations and acronyms

AES	Advanced Encryption Standard
AHS	Average of Effectively Applied Tariffs
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
ATPC	African Trade Policy Centre
BEREC	Body of European Regulators for Electronic Communications
BORCA	Botswana Communications Regulatory Authority
B2B	business to business
B2C	business to consumer
CABs	Conformity Assessment Bodies
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CIF	Cost, Insurance, Freight
CPC	Central Product Classification
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEPA	Digital Economy Partnership Agreement
DLT	distributed ledger transactions
DNS	domain name system
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSL	digital subscribers line
DTE	Digital Trade Estimates
DTRI	Digital Trade Restrictiveness Index
EAEU	Eurasian Economic Union
ECA	United Nations Economic Commission for Africa
ECC	Elliptic Curve Cryptography
ECLAC	United Nations Economic Commission for Latin America and the Caribbean
EE MRA	MRA for Electrical and Electronic Equipment
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ESCAP	United Nations Economic and Social Commission for Asia and the Pacific
ESO	electronic system operators
EU	European Union
FCC	Federation Communications Commissions
FDI	foreign direct investment
FIPS	Federal Information Processing Standard
FSS	Federal Security Service
GATS	WTO General Agreement on Trade in Services
GCI	Global Competitiveness Index
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications
GTA	Global Trade Alert
3GPP	3rd Generation Partnership Protection
HS	Harmonised System

HVAC	heating, ventilation, air conditioning
ICC	International Chamber of Commerce
ICLG	International Comparative legal Guides
ICPs	internet content providers
ICT	information and communication technology
ID	identity document
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IP	intellectual property
IPRs	intellectual property rights
ISO	International Organization for Standardization
ISPs	internet service providers
IT	information technology
I-TIP	Integrated Trade Intelligence Portal
ITIF	Information Technology and Innovation Foundation
ITU	International Telecommunication Union
LCRs	local content requirements
LCS	local carriage service
LSS	line sharing service
M&A	mergers and acquisitions
MFN	most-favoured nation
MLEC	Model Law on Electronic Commerce
MLES	Model Law on Electronic Signatures
MRA	Mutual Recognition Agreement
MSMEs	micro-, small- and medium enterprises
NIST	National Institute of Standards and Technology
NTE	National Trade Estimate Report
NTMs	Non-tariff measures
OECD	Organisation for Economic Co-operation and Development
PCT	Patent Cooperation Treaty
RDTII	Regional Digital Trade Integration Index
PECC	Pacific Economic Cooperation Council
RM	Malaysian ringgit
RMI	rights management information
SDoC	supplier declaration of conformity
SDR	special drawing rights
SIM	subscriber identity module
SMP	significant market power
SMEs	small and medium-sized enterprises
SOEs	state-owned enterprises
STRI	Services Trade Restrictiveness Index
TAPED	Trade Agreements Provisions on Electronic-commerce and Data
TDES	Triple Data Encryption Standard
TEL MRA	MRA for Conformity Assessment of Telecommunications Equipment
TGSB	The Gambia Standards Bureau
TIA	Telecommunication Industry Association

TLDs	Top-Level Domains
TPM	technological protection measure
TRAINS	Trade Analysis Information System
TRIPS	WTO Trade-Related Aspects of Intellectual Property Rights
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
URL	uniform resource locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WCO	World Customs Organization
WIPO	World Intellectual Property Organization
WITS	World Integrated Trade Solution
WTO	World Trade Organization
WTO GPA	WTO Government Procurement Agreement
WTO ITA	WTO Information Technology Agreement

Chapter 1

Conceptual framework

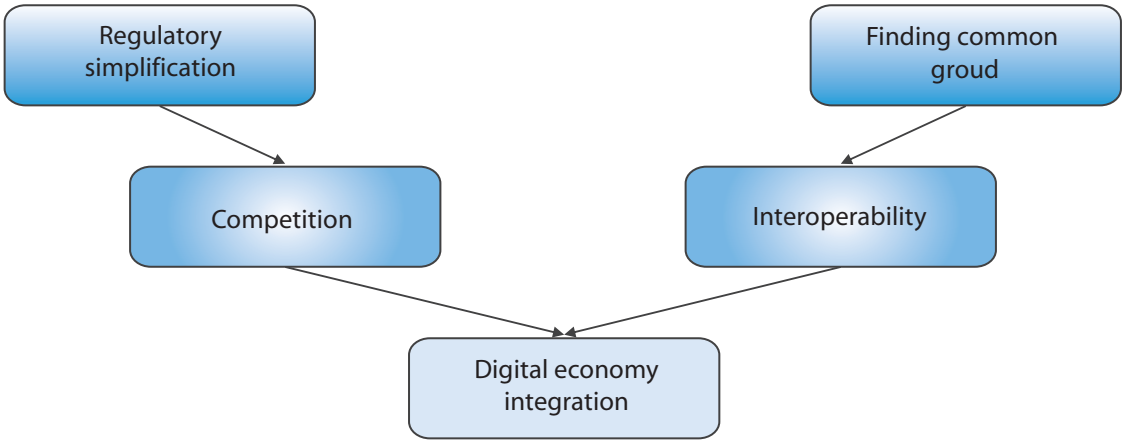
Background

Digital trade is defined as "digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered." (IMF, OECD, UNCTAD and WTO, 2023). Following the accelerated growth of digitalization, digital trade has increased significantly. Ketels and Bhattacharya (2019) estimated that up to 70% of all global trade flows could eventually be meaningfully affected by digitization, especially in service sectors. Policymakers have scrambled to assess the impact of this new way of doing business, and the policy and regulatory environment at the national and international level is evolving rapidly. A public consensus is that digital trade can facilitate digital economy integration in the region. However, reaping the opportunities brought by digital trade depends on government regulation of Information and Communication Technologies (ICT) products, digital goods and online services as well as trade intensity in each area of digital trade access to the Internet and other infrastructure related to digital trade.

Lowering regulatory compliance costs and enhancing interoperability as the basis for regional digital trade integration

The fewer trade and investment barriers and more simplification of the regulations in the region, the faster digital economy integration becomes. In this sense, the policy environment should not create unnecessary costs to the digital trade. Figure 1 summarizes the conceptual linkages between desired characteristics (regulatory simplification and interoperability) of the regulatory environment, and the ability to effectively trade and integrate into the digital economy. Regulatory simplification reduces compliance costs and as such encourages competition and spurs innovation. This will, in turn, increase productivity (Ferracane and others, 2019). At the same time, finding common ground with a wider practice of international standards will increase the interoperability of businesses that operate across different jurisdictions. It helps to lower the cost of compliance, especially for micro-, small- and medium-sized enterprises (MSMEs) (ABLI, 2020).

Figure 1 **Simplification and interoperability of digital trade rules**



The Regional Digital Trade Integration Index (RDTII) 2.0: Indicating the regulatory costs of doing regional business digitally.

The RDTII framework is a common framework developed in collaboration with the European University Institute and utilized by ESCAP, ECA and ECLAC for digital trade regulatory analysis for their member states in the Asia-Pacific, Africa, Latin America and the Caribbean regions. The framework is now in its second edition (RDTII 2.0), which improves upon its predecessor (RDTII 1.0) to enhance both comprehensiveness and clarity. It aims to informatively capture the potential for enhancing regulatory consistency through international and regional cooperation. Compared to the RDTII 1.0, the RDTII 2.0 features more detailed policy indicators, expanding the number of policy areas and increasing the number of policy indicators. Furthermore, the RDTII 2.0 framework has enhanced the clarity of its scoring criteria, facilitating data collection and policy evaluation in a manner that allows for more comparable analyses by different policy analysts.

The RDTII 2.0 framework identifies 12 policy areas, or "Pillars", to evaluate the regulatory environment affecting digital trade businesses (box 1 and figure 2). Each Pillar includes indicators that capture different elements and major policy measures under the Pillar. The index and indicator scores give a sense of the policy ecosystem facing digital trade businesses in an economy. The index scores, ranging from zero to one, imply how significant the regulatory environment adds to the cost of doing digital trade-related businesses. It is important to note that a high index score from heavy regulatory measures should not be interpreted as inherently bad. The implications depend on the context, perspective, and how the measures align with the goals and priorities of the stakeholders involved. In addition, the RDTII 2.0 framework considers that enhancing regional integration through more digital trade between the economies within the considered United Nations regions requires (a) promoting the interoperability of digital-trade regulatory approaches, (b) reducing the costs of regulatory compliance, and (c) promoting intraregional trade in goods and services that are important to the development of the digital economy, such as ICT goods and online services. Based on this principle, selected indicators address intraregional perspectives, such as those related to tariff and non-tariff measures imposed on intra-regional imports.

In this manner, RDTII 2.0 will help to identify regulatory areas of each economy in the region that need reconsideration to boost the competition and interoperability of digital trade. It is important to emphasize that the added costs are not necessarily trade impediments. Businesses can struggle with the high compliance costs of some forms of regulation while nevertheless fully recognizing the value and importance of regulations, such as privacy protection, to foster digital trust. However, a complex, ambiguous and heterogeneous regulatory environment can hamper trade. The index seeks to address the issues by considering indicators both for the lack of important legal frameworks and the risks of lacking interoperability. International treaties or model laws are used as benchmarks to assess regulatory interoperability.

It is important to note that digital trade governance is multi-faceted, which goes beyond the scope of the RDTII 2.0 framework. For example, some digital trade regulations may be shaped by policy objectives other than economic integration, growth and productivity, such as national security, data privacy, data protection and cybersecurity. While the public policy objectives are legitimate, the RDTII 2.0 framework aims to support policymakers in making informed policy decisions by highlighting the issue of compliance costs. Such costs tend to be fixed costs, which have disproportionate effects on small firms compared to large ones, and may be passed on to consumers. Additionally, they may stifle innovation and competition, especially in small markets.

Box 1

The RDTII 2.0 framework in brief

The overall RDTII 2.0 is a composite index integrating the scores of 12 pillars by using a simple average method. Each RDTII pillar score is the weighted average of scores at the indicator level.

The 12 pillars can be grouped into three broad clusters, which are traditional trade policies, other domestic policies and digital governance clusters. Specifically, the traditional trade policies cluster covers regulations such as non-tariff measures on ICT goods and services. The domestic policies cluster incorporates policies and regulations in broader policies, such as public procurement, telecom regulations and competition. The digital governance cluster encompasses modern domestic regulations that focus on data, Internet platforms and platform-generated transactions.

Indicator scores range from '0' to '1' and are based on a review of existing policies and regulations. A score greater than '0' indicates that at least one of the following conditions occurs:

- **Differential treatment** between domestic and foreign providers;
- **Additional regulatory compliance costs to services provided online**, relative to those provided offline;
- **Absence of certain international norms**, e.g., international agreement, legislation or legal mechanism considered to be of significant importance for interoperability across jurisdictions.

Pillar 1 covers **tariffs and trade defence** measures that limit trade in ICT goods with the Asia-Pacific partners.

Pillar 2 covers **restrictions on participation in public procurement** of ICT goods and services.

Pillar 3 covers **restrictions on foreign direct investment** in sectors related to digital trade. Such restrictions may be in place for national security and other legitimate reasons, but reduce competition.

Pillar 4 looks at **Intellectual Property Rights (IPRs) policies** and the balance between protecting individual rights to intellectual property and fostering innovation.

Pillar 5 covers policies and regulations regarding **telecommunications infrastructure and competition**.

Pillar 6 considers **cross-border data policies** which may address data privacy, data protection, data flows and other concerns, but also increase the costs of digital trade.

Pillar 7 covers **domestic data policies** governing the use of data in the regulating economy, such as regulations related to domestic data privacy, protection, retention and cybersecurity, that may enhance trust in digital transactions.

Pillar 8 deals with measures governing **Internet intermediary liability,** balancing the need for holding intermediaries responsible for illegal content over the Internet and not discouraging their participation in digital trade with onerous liability or obligations.

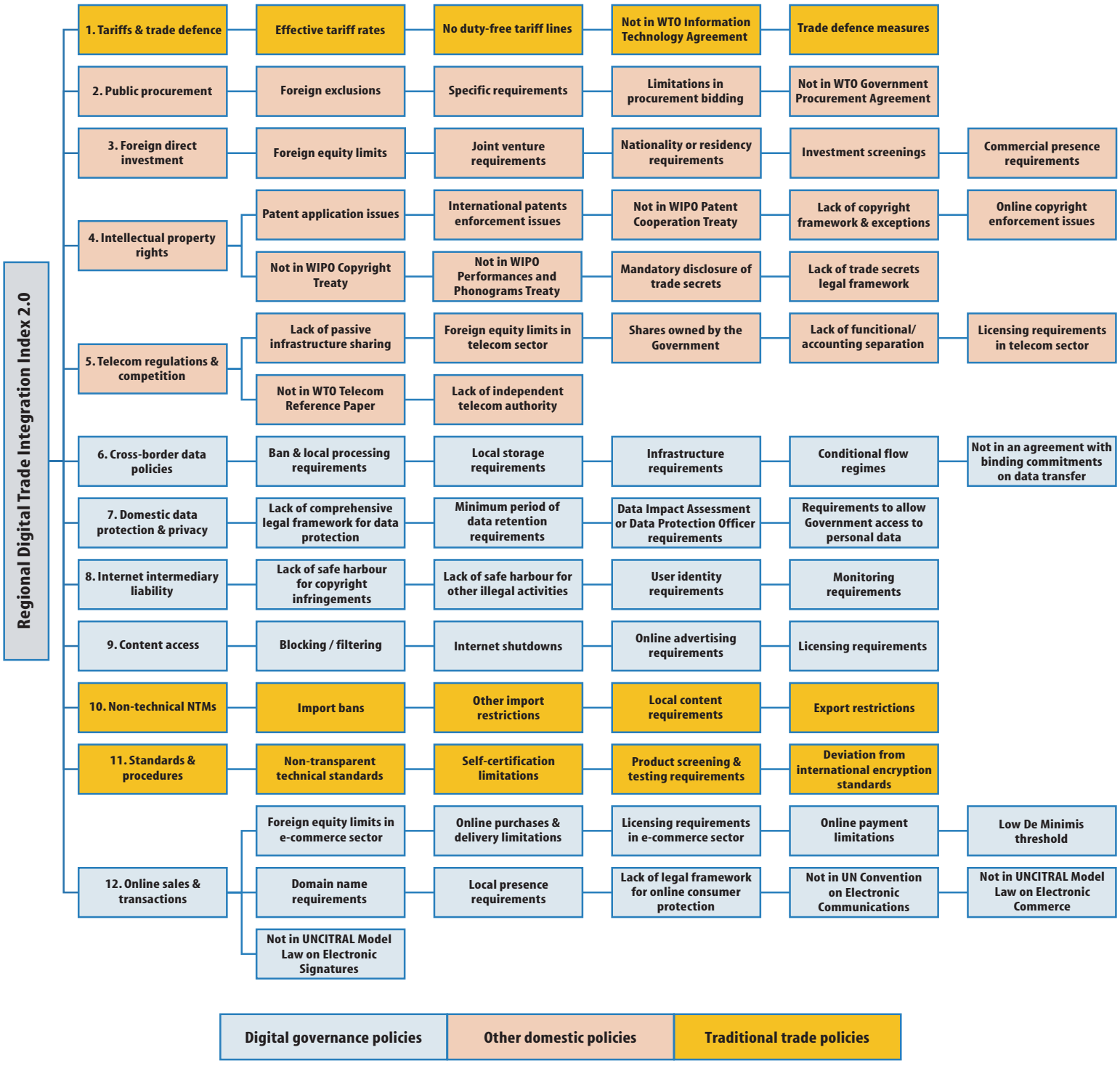
Pillar 9 deals with **content access,** balancing the interest to reduce illegal online content and the business costs for the intermediaries to conform with the requirements and the interruption to providing their services.

Pillar 10 captures non-technical measures (NTMs), including trade restrictions that are non-tariff measures (e.g., quotas) that limit the importation and exportation of ICT goods and online services from the economy in the Asia-Pacific region.

Pillar 11 focuses on **standard and related procedures**. This pillar considers procedural delays and complexity, which deviate from internationally recognized best practices, as a potential trade restriction for ICT goods and online services in the telecommunication sector.

Pillar 12 captures a broad spectrum of policies that affect **online sales and transactions**, including regulations on online purchase, delivery, online payment and domain names as well as legal recognition for electronic signatures and the existence of relevant consumer protection laws.

Figure 2 Regional Digital Trade Regulatory Integration Index (RDTII 2.0) – Pillars and indicators

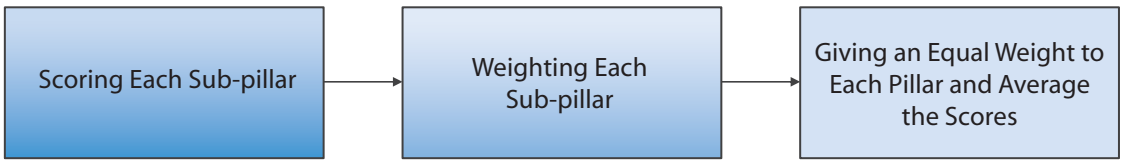


Chapter 2

RDTII 2.0 framework

The RDTII 2.0 identifies 12 policy domains or "Pillars" that shape the digital-trade regulatory environment. Each Pillar has policy indicators as proxies for the regulatory environment in respective policy areas. The indicators include those that capture different elements and major policy measures under the Pillar. Each indicator may have an impact on digital trade integration. Calculating a RDTII 2.0 score of an economy requires three steps by using a simple average method, as shown in figure 3: (a) apply a score for each indicator; (b) assign a weight for each indicator within a Pillar; and (c) give an equal weight for each Pillar and calculate the average of the scores from the Pillars to assign the RDTII 2.0 score to the economy.

Figure 3 **RDTII 2.0 methodology**



Scoring methodology

The RDTII 2.0 illustrates the interoperability of regulatory regimes within and across regions in terms of trade and compliance costs for business. For this purpose, the score in each indicator varies between '0' (low compliance cost) to '1' (high compliance cost). As such, implying the score shows how much the regulatory environment adds to the 'cost of doing digital trade-related business'. A score above '0' indicates one of the following conditions:

First, a measure implies **a differential treatment** between domestic and foreign providers of ICT goods or online services. For example:

- A public procurement that is only accessible to national companies. It may serve the interest of protecting the domestic market, but it *blocks* foreigners from participating in the procurement.

Second, a measure that aims at achieving a non-economic objective but may end up adding **regulatory compliance costs to businesses**. Such measures sometimes affect not only foreign businesses but also domestic businesses. For example:

- A measure that requires both foreign and domestic entities bidding for public procurement to submit trade secrets or to use a specific encryption standard. While this may increase cybersecurity, it discourages firms from submitting a bid due to the fear of technology transfer or additional costs for reconfiguration.

Third, a country does **not follow certain international norms**, or is a member of international agreements, legislations or legal mechanisms that enhance interoperability across jurisdictions. For example:

- Signatory to the WTO Information Technology Agreement;
- Signatory to the WTO Agreement on Government Procurement;
- The doctrine of fair use;
- Legislation for data protection;
- Safe-harbour provisions for Internet intermediaries;
- Legislation for electronic transactions and signatures.

Weighting indicators

To generate a score from a Pillar, RDTII 2.0 takes an unweighted approach across the 12 Pillars and a weighted approach to the indicators within each Pillar. The weights given to each indicator come from the study on the Digital Trade Restrictiveness Index (DTRI) of the European Centre for International Political Economy, which was conducted in 2018. The study indicates that weights given to each indicator reflect the expert opinions on the importance of each indicator within the considered Pillar (Ferracane and others, 2019). In other words, a higher weight is given to an indicator capturing measures that tend to have high impacts on digital trade based on expert opinion. For example, the indicators of import bans and local content requirements under Pillar 9 capture non-technical NTMs. An import ban blocks certain imports *per se*, thereby being given a higher weight than a local content requirement, which allows imports as long as they are composed of domestic components.

Averaging the scores in each Pillar to generate RDTII 2.0 scores

While RDTII 2.0 applies unequal weights to the indicators within each pillar, it applies an equal weight on each pillar to produce a final RDTII 2.0 score for an economy. The composite RDTII 2.0 runs from 0 (low compliance cost) to 1 (high compliance cost).[1]

Avoiding double scoring

A regulatory measure can have impacts across several policy areas. In certain situations, a single regulatory measure may address multiple RDTII 2.0 indicators. For example, a law requiring licences for digital platforms that include online marketplaces, car sharing, social media etc., affects both digital applications and e-commerce businesses. This law will be evaluated under the following indicators: Licensing Schemes for Digital Content Providers, Digital Services, and Applications (Pillar 9.4), and E-commerce Licence (Pillar 12.3). This is because the law has an impact both on digital applications and on e-commerce businesses.

Scoring is typically based on the nature (conditions) of the measure. When a measure is captured in several indicators, the researchers should record the measure in all relevant indicators for reference purposes but must avoid double counting the policy conditions.

For example, a condition to obtain a licence for operating an e-commerce business that includes establishing a branch or office in the host economy should be recorded under E-commerce Licence (Pillar 12.3) and Commercial Presence Requirement (Pillar 3.5). However, it should be scored only once, at Pillar 3.5, because the nature of this licence is a commercial presence requirement.

[1] It takes an equal-weighting approach to the pillars because it is not as straightforward to compare the importance of different pillars. For example, it is not evident whether domestic data policies have more substantial impacts than FDI policies.

Sources of regulatory measures

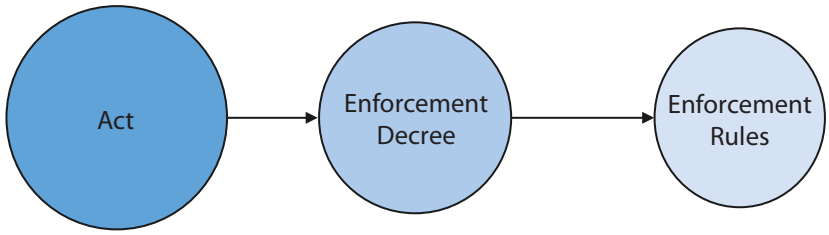
Researchers should look at the official gazette of laws, regulations, official guidelines, official government reports and other measures to find relevant information for each indicator. Secondary sources such as reports, publications, news and legal reviews serve only to guide researchers' attention to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration. Examples of useful secondary sources are provided under each indicator later in this document.

However, there are two potential challenges in finding relevant information.

First, there may be a gap between what the law says (*de jure*) and how that law applies (*de facto*). Usually, this results from (a) considerable discretion in decision-making and implementation of regulation, and (b) a lack of transparency on institutional structures.

The second challenge is that fine-grain regulatory detail is not always available. To address this challenge, researchers should dig deeper into the hierarchy of law: statutes – regulations, decrees, decisions and so on. For example, for the Republic of Korea, the hierarchy of legal instruments runs from Acts to Enforcement Decrees and then Enforcement Rules, as shown in figure 4. The Enforcement Decrees and Rules, which are promulgated by administrative agencies, spell out in detail what Acts mandate, which are enacted by the legislature.

Figure 4 **Republic of Korea's regulatory measures**



Lack of regulatory measures

In cases where there is no measure relevant for an indicator, researchers should note the lack of measures and insert the relevant general rules for that indicator. For example, the indicators of Pillar 2 capture restrictions on foreign participation in public procurement. If a respective economy does not impose any captured restrictions, the researchers should cite the Public Procurement Act or other regulations governing public procurement in the respective economy as reference.

Chapter 3

RDTII 2.0 pillars

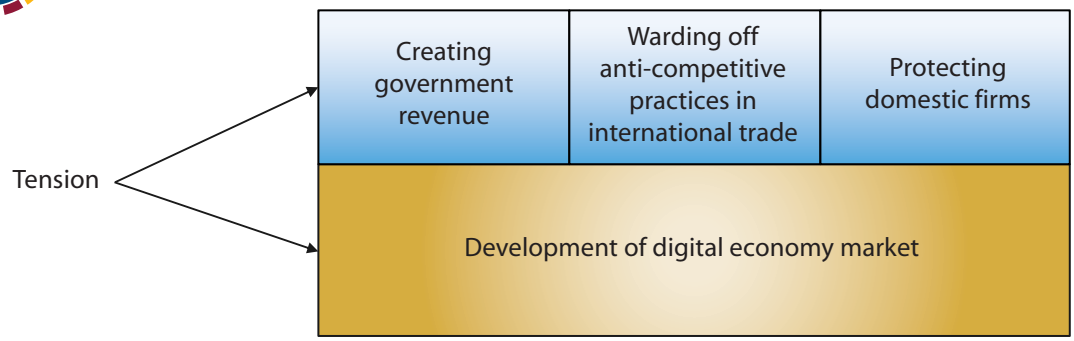
Pillar 1. Tariffs and trade defence

Pillar 1 covers tariffs and trade defence measures applied to intraregional imports of ICT goods. ICT products or ICT goods are final goods whose main purpose is to capture, transmit, process, and render information and intermediate goods and inputs that are crucial to manufacturing these goods. Examples include smartphones, computers, network equipment, storage media, semiconductors, electrical parts, electronics, sensors, processors and cables. The RDTII 2.0 results are based on ICT products under WTO Information Technology Agreement (ITA) I and ITA II, as well as the proposed ITA III expansion by the Information Technology and Innovation Foundation (ITIF) (see Annex II).[2]

As figure 5 reveals, these measures are often designed to protect domestic firms, provide a source of government revenue, and counteract anti-competitive practices taken by foreign firms or foreign Governments. However, the measures have risks of limiting the development of the digital economy market. For example, tariff measures on electronics, telecommunication items and high- performance computing technologies may reduce an economy's exposure to advanced digital products or technologies, thereby deepening digital divides (Ferracane and others, 2019). Furthermore, tariffs and trade measures on basic materials for batteries and hardware as well as finished products such as computers, electronics and telecommunication equipment affect the costs of digital trade.

Figure 5

Tension among different policy objectives in Pillar 1



Pillar 1 measures consider the following areas:

- Effectively applied tariffs on ICT goods (in weighted average) imported from other economies within the considered United Nations region;
- No duty-free tariff lines on ICT goods from other economies within the considered United Nations region;
- Not in the WTO Information Technology Agreement (ITA) of 1996 (ITA I) and its expansion in 2015 (ITA II); and
- Trade defence measures including anti-dumping, countervailing duties and safeguards on ICT-related goods imported by other economies within the considered United Nations region.

[2] The RDTII 2.0 results are based on the list of ICT products found in the "ITA 3.0" list proposed by the Information Technology and Innovation Foundation (ITIF) 2021 (Ezell and Dascoli, 2021). The ITA 3.0 includes all products under the WTO's Information Technology Agreement (ITA) I and ITA II products as well as additional products provided by the ITIF (see Annex II). The proposed WTO ITA III expansion includes next-generation ICT products, such as robots, 3D printers, drones, certain medical technologies, and unmanned aerial vehicles.

Effectively applied tariffs on ICT goods (in weighted average) imported from other economies within the considered United Nations region

This indicator is the weighted average of effectively applied tariffs (AHS)[3] of each reporting economy to the rest of the economies within the considered United Nations region (e.g., Viet Nam effectively applied tariffs to the rest of the ESCAP (Asia-Pacific) region). Effectively applied tariffs are defined by the World Integrated Trade Solution (WITS) as the lowest available tariffs. If a preferential tariff rate exists, it will be used as the effectively applied tariff. Otherwise, a most-favoured nation (MFN) applied tariff will be used. The reason why the AHS also incorporates the preferential tariff is that the index seeks to measure the actual level of tariffs applied to the ICT goods (the WTO ITA I, ITA II, and the proposed ITA III expansion) from regional partners considered. Using the MFN tariff alone would only provide a picture of the highest tariff rates imposed.

The reason why the index uses the weighted average rather than the simple average rates is that the simple average does not account for the relative importance of digital goods in terms of their trade volumes. The weighted average accounts for this relative importance by weighing each tariff rate by the share of the trade volumes of each tariff line. This means that tariff rates of digital goods with higher trade shares get higher weights than tariff rates of digital goods with lower trade shares.

To normalize the tariff rates into the score between zero and 1, the score calculation follows a linear function of f(x) = 0.1x, where x is the weighted average tariff rate on ICT goods. If the average tariff rate is within the range of zero and 10%, the score will be less than '1,' while any tariff rate higher than 10% will be scored at '1'. For example, an economy with an average tariff of 1% receives a score of '0.1', while another economy with an average tariff of 10% or higher receives a score of '1.'

The data for average tariff rates are found in the WITS database. For the specific steps to find the data for zero-tariff lines, refer to Annex I.

No duty-free tariff lines on ICT goods imported from other economies within the considered United Nations region

The second indicator is the no duty-free tariff lines or coverage rate of zero-tariffs that apply to ICT goods (the WTO ITA I, ITA II, and the proposed ITA III expansion) imported from other economies within the considered region. The indicator follows a linear function, f(x) = -0.025x + 1.75, where x is the coverage rate calculated from the number of free tariff lines for ICT goods divided by the total number of tariff lines for ICT goods, multiplied by 100. However, when the coverage rate is 30% or below, the score will be truncated to '1.' In contrast, when the duty-free coverage rate are greater than 70%, the score will be truncated to '0'. The data for zero-tariff lines in a given economy is found in the WITS database. For the specific steps to find the data for zero-tariff lines, refer to Annex I.

Not in the WTO Information Technology Agreement (ITA I or ITA II)

This indicator looks at whether economies are members of the WTO's ITA I ("the Ministerial Declaration on Trade in Information Technology Products") or ITA II ("the Ministerial Declaration

[3] For more information about the different types of tariffs, please visit the WITS website: https://wits.worldbank.org/wits/wits/witshelp/content/data_retrieval/p/intro/c2.types_of_tariffs.htm.

on the Expansion of Trade in Information Technology Products"). The ITA I requires its members to "eliminate and bind customs duties at zero for all products specified in the Agreement."[4] In ITA II, the members agreed to expand the products covered by the ITA I by eliminating tariffs on an additional list of 201 products.[5]

The ITA I and II are a close proxy for tariff measures that apply to ICT products. The WTO reports that, today, ICT products account for approximately 10% of global merchandise exports (WTO, 2001). ICT products covered by the ITA I alone account for approximately 97% of world trade in the IT sector. The expanded list of the products under ITA II accounts for approximately 7% of total global trade today.

The reason why the index includes this indicator, even though it already takes into account the coverage rate of zero-tariff on ICT products, is that the schedules of concessions bind the economies to their obligations to other members under the agreements, unlike domestic policies of zero tariffs. Because the members would have the legal obligation not to impose import duties on the covered products, investors and traders would benefit significantly from improved market access, predictability and certainty (WTO, 2001).

The score is '0' if an economy has signed both agreements. If an economy signed only ITA I, the score is '0.5.' If an economy signed neither of them, the score is '1.'

To see participants in the Agreement, check the WTO official site. Specifically, to check whether the economies have ITA II membership, the official government website, the WTO Ministerial Declaration on the Expansion of Trade in Information Technology Products 2015, and the information provided on the WTO official site are useful sources. The WTO Trade Policy Reviews are also a useful secondary source. The secondary source should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Trade defence measures including anti-dumping, countervailing duties and safeguards on ICT-related goods imported by other economies within the considered United Nations region

The indicator looks at whether an economy is enforcing trade defence measures such as anti- dumping duties, countervailing duties and safeguard measures against ICT-related goods imported from any economy in the considered region.[6] Only the active measures will be counted, while efforts of investigation measures in the pre-implementation stage or terminated measures will be not counted. For example:

- Japan imposes duty on imports of electrolytic manganese dioxide, which is a component of batteries originating in China, from 34% to 46% depending on the company;

[4] The ITA concessions are included in the participants' WTO schedules of concessions, and the tariff elimination is implemented on a MFN basis (WTO, 2001). This means that even economies that have not joined the ITA can benefit from the trade opportunities generated by ITA tariff elimination.

[5] For the list of products cover under the WTO's ITA I and ITA II see Annex II.

[6] In the case of Latin America, RDTII 2.0 only includes trade defence measures on products from China (e.g., in Argentina, Brazil and Mexico).

- India imposes an anti-dumping measure on imports of electrical insulators and polytetrafluoroethylene used for wiring computer applications originating in China;
- Argentina imposes an anti-dumping duty on imports of electrical connection terminals from China and Germany;
- Brazil imposes a definitive anti-dumping duty on imports of loudspeakers from China;
- Türkiye imposes an anti-dumping duty on welded stainless-steel tubes, pipes and profiles (HS code 560311) originating in Viet Nam, with duty rates of between 19.64% to 25% of the CIF, depending on the company.

For each measure, the economy receives '0.25', with '1' being the maximum score in this indicator. Thus, if an economy is enforcing four or more than four of such measures, it receives '1'. The score is '0' when trade defence measure is not enforced.

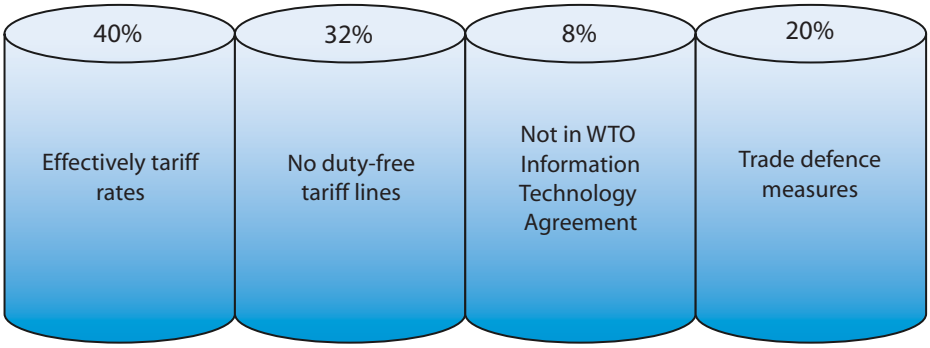
For sources, find WTO members anti-dumping notifications under the agreement on implementation of Article VI of GATT 1994 ("G/ADP/N/1/…"), notifications relating to countervailing measures or the most recent official gazette of a relevant national ministry. Useful secondary sources include the Integrated Trade Intelligence Portal (I- TIP) and the Global Trade Alert (GTA) database. The secondary sources should serve only to guide researchers' attention to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

The weights for each indicator

As shown in figure 6, weight rates of 40%, 32%, 8% and 20% are given to the indicators, respectively. The first and the second indicators on tariffs applied on ICT goods are given great weight of 40% and 32%. This is because the tariffs (or lack thereof) on ICT products reflect a comprehensive impact on costs of digital trade in ICT products, whereas the trade defence measures sporadically apply to a few sets of imports, hence being given lesser weight of 20%. Furthermore, the fact that an economy is not a member of the WTO ITA I or II does not mean that its tariff rates are restrictive, as long as the economy does not impose tariffs on a number of ICT products; thus, the last indicator was given least weight of 8%.

Figure 6

Pillar 1 indicators and the weights



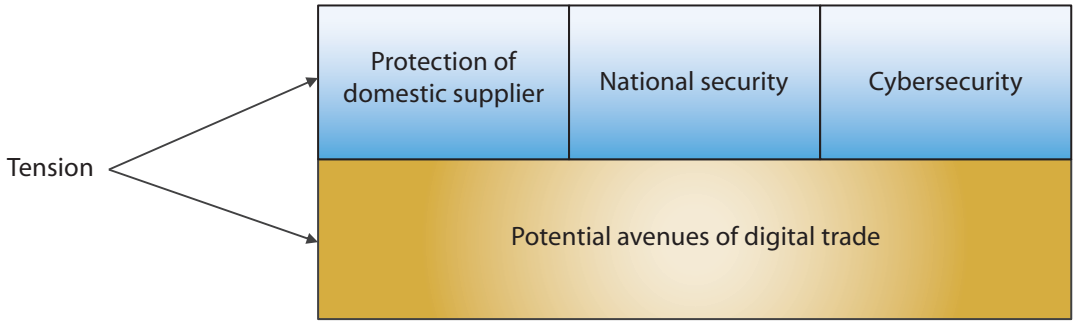
Pillar 2. Public procurement

Pillar 2 covers measures on public procurement related to ICT goods and online services. Public procurement is generally applied to various sectors, including the sectors related to digital trade, affecting ICT goods and online services. There is tension among different policy objectives in procurement policies, as shown in figure 7. It investigates whether domestic bidders tend to have an advantage in government procurement. Specifically, for procurement in sectors relevant to digital trade, such as IT technologies and infrastructure, national security and cybersecurity interests may be involved in forming procurement policies as procuring entities carry sensitive information in the operation of public administration.

However, some measures that exclude foreign suppliers in government procurement block potential avenues of digital trade. Accordingly, while the national security and cyber security interests are significant, economies need to examine whether the measures are necessary to serve those interests or other less restrictive means exist.

Figure 7

Tension among different policy objectives in Pillar 2



Based on this understanding, Pillar 2 covers discriminatory measures or measures with high compliance costs. Specifically, the Pillar does so by looking at:

- Foreign exclusions from public procurement;
- Specific requirements on source codes, encryption and trade secrets;
- Limitations in procurement bidding; and
- Not in the WTO Government Procurement Agreement (GPA).

For this Pillar, useful secondary sources include the OECD Services Trade Restrictiveness Index (STRI) Regulatory Database, the USTR National Trade Estimates (NTE) Report and the GTA database. The secondary sources should only serve to guide researchers to the primary sources (i.e., actual laws, regulations and official documents issued by Governments). In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Foreign exclusions from public procurement

This indicator covers measures that may exclude foreign enterprises from public procurement, including for ICT goods and online services. The exclusion of foreign firms in public procurement not only discriminates against foreign firms but also limits the opportunity of the domestic economy to access new digital technologies that foreign firms could offer. The exclusion can take various forms:

- Foreign enterprises are not allowed to participate in the public procurement of certain ICT goods and online services. For example, the Russian Federation imposes a two-year prohibition on the procurement of memory storage devices from foreign countries for governmental and municipal needs;
- Foreign enterprises can only take part in public tenders when domestic service suppliers are not participating or available. For example, Malaysia and Viet Nam only accept foreign suppliers when local goods and services are not available. Nepal accepts international bidding in public procurement when goods cannot be procured at competitive price, when there is no national bid has been submitted or when the goods to be procured are certified by a public entity as complex and special nature;
- Foreign enterprises can participate in public procurement when the foreign enterprises are required to bid in cooperation with the domestic enterprises. For example, Thailand requires foreign consultants to team up with domestic ones to participate in public tender.

A country receives a score of '1' if it excludes foreign enterprises from public procurement. The score is also '1' if there is an instance where an economy has excluded two or more specific (groups of) foreign firms from public procurement. The score of '0.5' is assigned when there is an instance where an economy has excluded a specific (group) of foreign firm(s) from public procurement. The score is '0' if no such measure exists.

Specific requirements on source code, encryption and trade secrets

The indicator asks: (a) whether firms are required to surrender source code, encryption and other trade secrets such as patents as a condition for successful public procurement and (b) whether firms are required to use a specific encryption standard to be successful for their bidding.

A requirement to transfer technology or use a specific encryption standard in public procurement often stems from interest in protecting national security. However, these types of requirements may prevent foreign companies from entering the domestic market because of concern about the disclosure of their trade secrets and increasing costs of configuration with a new system. For example:

- Indonesia requires that providers of custom-made software must provide or escrow the source codes associated with their service;
- The Philippines requires technology and knowledge transfer to the procuring entity for the provision of consulting services;
- India prescribes certain modes or methods for encryption for e-government and e-commerce procurement;

- The Republic of Korea requires suppliers of software, network and hardware equipment that deals with "non-confidential but important information" to comply with the Cryptographic Module Validation Standards, encryption standards developed in the Republic of Korea (e.g., ARIA, SEED, LEA and Hight);
- In Egypt, the use of encryption requires the approval of the National Telecom Regulatory Authority as well as the armed forces and national security entities.

The score is '1' if there is a requirement to surrender such trade secrets as a condition for participating in tenders. The score is '0.5' if firms are required to use specific encryption to win tenders. The score is '0' if there is no such measure.

For this particular indicator, the World Map of Encryption Laws and Policies is a useful secondary source. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Limitations in procurement bidding

This indicator covers limitations on participation in public procurement. These limitations can take various forms: (a) a ban on participation in public procurement; (b) allocation of a quota; (c) preference in favour of certain suppliers; and (d) price preference in favour of certain suppliers. These limitations trigger when certain conditions are met, which include: (a) nationality of suppliers; (b) other status such as being SMEs or indigenous; and (c) percentage of local content in supplies. For example:

- Brunei Darussalam bans participation in ICT public procurement of suppliers who do not meet local-content requirements;
- India retains a quota of 25% of the annual value of goods or services from Indian SMEs;
- Nepal gives preference to domestic firms or firms that participate in joint ventures with domestic firms, organizations or companies;
- Rwanda imposes local content requirements giving a 15% preference to goods produced locally and a 10% preference to bidders registered in Rwanda;
- Nigeria's Guidelines on Content Development in ICT requires that Ministries and other government entities purchase all hardware products locally as well as source and procure software from only local and indigenous software development companies. If the capacity for developing such software does not exist locally, a Nigerian company should provide the procurement, installation and support of the software;
- According to Supreme Decree No. 27,328, public calls for national purchases of up to approximately US$ 1,166,000 is directed to national production companies that are legally established in Bolivia. Foreign companies are excluded unless there are no national providers available;
- Malaysia provides price preference to domestic bidders by a certain margin, depending on the value of their suppliers. For example, for suppliers and services contracts between RM 100,000 (US$ 23,500) and RM 15 million (US$ 3.5 million), the margin of preference is between 2.5% and 10%, and is inversely proportional to the value;

- Argentina's Law 27,328 establishes that in public-private partnership contracts, at least 33% of the goods and services used must be provided by local companies.

The ban on participation in procurement based on nationality or other status blocks international trade *per se*, whereas other limitations such as the allocation of a quota and preference schemes discourage, if not block, international trade in procurement in sectors relevant to digital trade.

To categorize a measure accordingly, the first step is to identify the effect of a measure, i.e., ban, quota, preference and price preference; the second step is to identify the condition upon which the measure takes effect, i.e., nationality, other status and local content percentage.

The score is '1' for a measure that bans participation in public procurement based on nationality or other status, or if two or more requirements of the '0.5' category apply. The score is '0.5' if there is a measure that bans the participation unless a local content requirement is met, if there is a quota or a preference scheme given only to suppliers who meet certain conditions such as nationality, other status or a local content percentage, or if there is lack of institutional transparency in public procurement. The score is '0' if none of the above measures exist and there is institutional transparency.

Not in the WTO Agreement on Government Procurement (GPA)

This indicator looks at whether an economy is a signatory to the WTO's GPA (box 2). The GPA is a plurilateral agreement (WTO, 2000). The Agreement ensures the principle of non- discrimination in public procurement by committing its members according to the most-favoured-nation treatment and national treatment. However, these rules are subject to each party's coverage schedule (Annex V regarding services of the GPA)[7] that determines whether procurement activities in a particular sector are covered by the Agreement or not.

The score is '1' if an economy is not a member of the GPA or if an economy's coverage schedule does not cover any one of telecommunication services (CPC 752), telecommunications-related services (CPC 754), and computer and related services (CPC 84). The score is '0' if an economy, a member of the GPA, fully covers these service sectors related to digital trade (United Nations, 1991). Each party's coverage schedule can be found on the e-GPA Portal.

[7] Available at https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm

Box 2

The Agreement on Government Procurement (GPA)

The GPA is a plurilateral agreement within the framework of the WTO, meaning that not all WTO members are parties to the Agreement. At present, the Agreement has 21 parties comprising 48 WTO members (counting the European Union and its 27 member States as one party). Not long after the implementation of the GPA in 1994, the GPA parties initiated the renegotiation of the Agreement. The negotiation was formally adopted and came into force for all those parties to the GPA 1994 that had ratified the GPA 2012, while allowing other parties to the GPA 1994 to continue completing their domestic ratification procedures. The last of those other parties, Switzerland, completed the ratification in 2020, and the GPA 2012 replaced the GPA 1994.

The ultimate aim of the Agreement is to mutually open government procurement markets among its parties by progressively reducing and eliminating discriminatory measures and achieving the greatest possible expansion of the coverage. According to the WTO, the GPA parties have opened procurement activities estimated to be worth more than US$ 1.7 trillion annually to international competition.

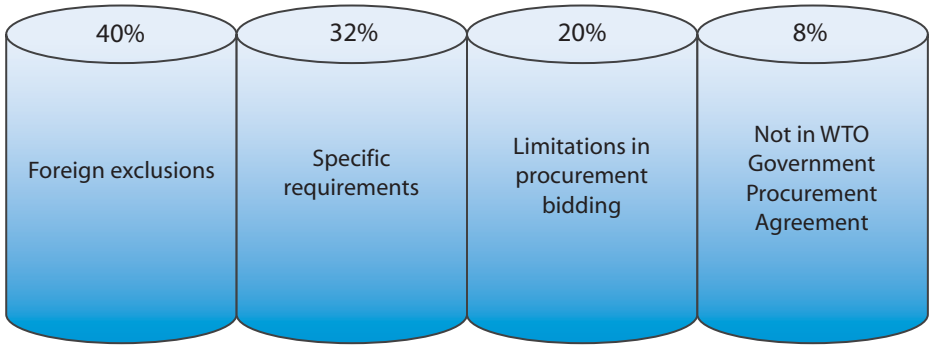
The GPA is composed mainly of the text of the Agreement and the parties' market access schedules of commitments. The text of the Agreement establishes rules mandating that open, fair and transparent conditions of competition be ensured in government procurement in member economies. However, these rules do not automatically apply to all procurement activities of each party; rather, the coverage schedules of each party determine whether a procurement activity is covered by the Agreement or not. Only those procurement activities that are carried out by covered entities purchasing listed goods, services or construction services of a value exceeding specified threshold values are covered by the Agreement.

The weights for each indicator

As shown in figure 8, weights for each indicator are 40%, 32%, 20% and 8%, respectively. The exclusion of foreign firms from procurement receives the most significant weight of 40% because it discriminates against foreign firms and *per se* bans foreign participation in public procurement. The requirements regarding trade secrets and other limitations on participating in procurement receive a lesser weight because they do not discriminate against foreign firms. Specific requirements to surrender source code, encryption and trade secrets are assigned a greater weight (32%) than the limitations on participating in procurement (20%). Although both indicators discourage a company from participating in public procurement, the specific requirements including mandatory disclosure of trade secrets affect the business's economic value and competition. The WTO GPA requires additional commitments of the most-favoured nation treatment and national treatment for procurement. However, not being a signatory of the treaty does not necessarily mean that the economy has a measure that discriminates against foreign firms or adds regulatory compliance costs in procurement. Therefore, the weight of this indicator is less than the others (8%).

Figure 8

Pillar 2 indicators and the weights

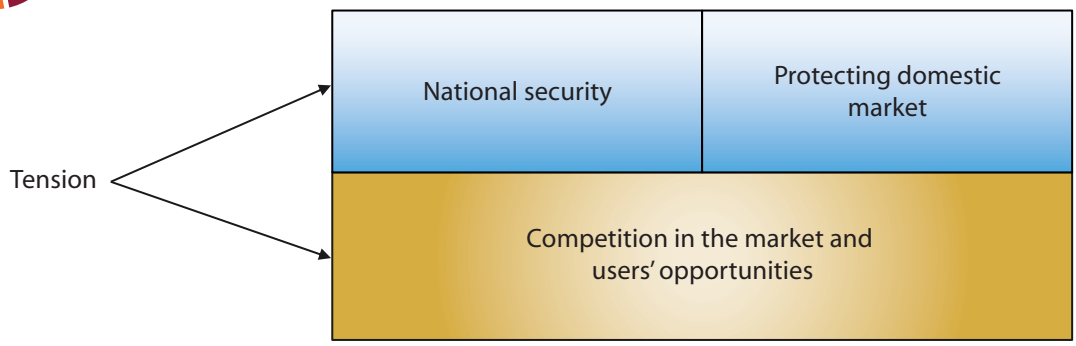


Pillar 3. Foreign direct investment

Pillar 3 covers measures on foreign direct investment (FDI) in sectors related to digital trade. These sectors include the manufacturing of telecommunication facilities, telecommunication services, computer services and Internet services.

Tensions in public and FDI policies may exist between the interests to protect national security and the domestic market and the need to attract FDI (figure 9). Furthermore, as much as telecommunication facilities, networks and other related services are critical, economies may not want to increase their dependence on foreign investors in these sectors. However, some foreign investment measures do not necessarily address these concerns but may risk restricting foreign investment, reducing competition in the market, and limiting users' opportunities to access better quality goods and services.

Figure 9 **Tension among different policy objectives in Pillar 3**



In this regard, Pillar 3 covers conditions in foreign investment policy that may create a burden on foreign investors. Indicators in this Pillar consider the following requirements:

- Foreign equity limits;
- Joint venture requirements;
- Nationality or residency requirements for board of directors or managers;
- Investment screening; and
- Commercial presence requirements.

For sources, these measures are found in laws governing companies, foreign investment or sectoral laws (e.g., telecommunications laws). Useful secondary sources include the latest NTE report by the U.S. Office of Trade Representative, the latest Investment Climate Statements by the U.S. Department of State, the OECD STRI database, and the GTA database. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Foreign equity limits

This indicator concerns maximum foreign equity shares in sectors related to digital trade, including limitations on shares in government-controlled companies. Foreign equity shares are shares that foreign natural or legal persons hold in a firm incorporated in the investee economy. Limitation on foreign equity shares is a direct obstacle for foreign investors that could induce a higher level of development in the sectors. The foreign equity shares under this Pillar focuses on foreign equity shares applied horizontally to all sectors or specific sectors relevant to digital trade, except telecommunication and e-commerce sectors where they are captured separately under Pillars 5 and 12.[8]

The score is '1' if there is a ban on foreign ownership in at least one sector or if only a minority stake (less than 50%) is allowed in more than one sector. The score is '0.8' if only a minority stake is allowed in one relevant sector. The score is '0.5' where a controlling stake (more than 50%) is allowed, but maximum caps on foreign equity exist or where limitations on foreign equity shares only exist in state-owned enterprises (SOEs). The score is '0' if there is no limitation on foreign equity share in relevant sectors.

Joint venture requirements

This indicator asks whether there is a requirement for firms to engage in a joint venture with a local firm in order to invest or operate in the economy. While forming a joint venture with a domestic firm helps foreign investors to strategize business effectively in a market unfamiliar to them and navigate through domestic regulation, the investors are in a better position than the Government to determine whether a joint venture is necessary. Furthermore, a mandatory requirement to form a joint venture with a domestic partner can discourage foreign investors due to the concern that technology might be forcefully transferred. Examples of joint venture requirements are:

- China, which requires all foreign providers of a data centre or cloud computing services to form a joint venture with Chinese firms;
- Indonesia, which requires providers of consultancy services for the installation of computer hardware or software implementation to form a joint venture with a local firm;
- Vanuatu, which requires foreign firms that undergo "expansion" more than three times to form a joint partnership with a citizen of Vanuatu;
- Egypt requires a joint venture for companies operating in trade sector projects, with possible exceptions for projects in remote areas;
- Supreme Decree No. 27,328 of Bolivia states that international companies can only participate in partnership with local consulting firms.
- Liberia's Investment Act requires a joint venture or partnership between a Liberian and a foreigner to invest in a few businesses (commercial printing, advertising, graphics and commercial artists) if the total shareholding of the Liberian is at least 25% and the total capital invested is not less than US$ 300,000.

If there is one of these measures, the score is '1.' Otherwise, the score is '0.'

[8] Certain economies implement specific regulations for the telecommunication sector and e-commerce sector. In particular, the telecommunication sector is regulated by the sectoral regulators; thereby, these regulators have jurisdiction over such matters.

Nationality or residency requirements for the board of directors or managers in sectors relevant to digital trade

This indicator asks whether there are nationality or residency requirements for members of the board of directors or managers. These measures prevent foreign investors from appointing board members or managers of their choice.[9]

- Nationality requirements. For example, Japan prohibits foreigners from being a board member in telecom companies. Thailand requires that the majority of the board of directors of the telecommunication business must have Thai nationality. Indonesia specifies that 19 positions, including directors, managers and supervisors, are reserved for Indonesian nationality; and
- Residency requirements. For example, the Philippines mandates a residency requirement for treasurer and secretary. Singapore requires that a company must have at least one director who is ordinarily resident in Singapore.

If there is any requirement that at least one member of the board of directors or a manager has to reside in the economy or be a national of the economy, the score '1.' Otherwise, the score is '0.'

Investment screenings

This indicator asks whether (a) an economy has adopted any screening mechanism for foreign investment or mergers and acquisitions (M&A) in sectors relevant to digital trade, excluding those implemented solely for antitrust purposes, unless such mechanisms are found to be discriminatory; and (b) the potential impacts of these screening mechanisms on blocking foreign investment and M&A in sectors relevant to digital trade.

The mechanisms primarily are based on either the interests of national security and public order or purely economic interest. Even the screening mechanisms that refer to economic interest, conditions and criteria are often unclear. The process mostly applies in a discretionary manner, creating uncertainty for investors and potentially discouraging investment activities. It is challenging to declare that screening mechanisms based on national security interests are less justified than those based on economic interest or vice versa.

Regardless of the interests, the screening requirement is categorized by the potential impact on investment. For example, an investment-screening measure that has a potential to block investment includes the cases that the Government is authorized to exercise call-in powers based on the amorphous national or security interests, and explicit differential treatment between foreign and local investor in investment screening. Examples of the screening mechanisms that potentially block trade in sectors relevant to the digital trade are:

- Australia screens out investment actions that are contrary to national interest in sensitive sectors such as infrastructure, telecommunications and media. The economy also has a backup mechanism that may screen out investment activities in other sectors by creating a "call-in" power. Previously approved investment activities could be open to re-assessment;

[9] Residency or nationality requirements that apply only to officers who are not directors or managers do not count under this sub-pillar.

- The Dominican Republic states that administrators, managers, directors and other persons in administrative or management functions must preferably be of Dominican nationality. In addition, at least 80% of the total number of workers of a company must be composed of Dominicans.
- New Zealand applies a three-stage investment screening process. First, a foreign investor in a significant business asset (an investment activity that results in a 25% or greater ownership or whose value exceeds US$ 71 million) must obtain consent. Second, a foreign investment in strategically important business, such as telecommunication infrastructure and media entities, can be subjected to the national interest test and the consent may be declined if a transaction is contrary to national interest. Third, investment is subjected to 'call in transaction' under which the Government may block, impose conditions on, or order disposal of the activities if they pose a threat to national security or public order.
- Viet Nam grants the authority to review and halt foreign investments on the grounds of national security. The terms "national defence" and "security" are not clearly defined in the law.

Examples of other cases of screening mechanisms in sectors relevant to the digital trade include:

- In Mexico, the National Commission of Foreign Investment evaluates whether foreign investment applications meet certain criteria, including the impact on employment and workers' training, technological contribution and an increase in the competitivity of the economy. This Commission can prevent acquisitions by foreign investment for reasons of national security;
- Vanuatu conditions its approval of investment activities on the provision of employment to locals and local capacity-building;
- Cameroon has a screening process applicable to all domestic and foreign investments that ensures that investors meet the criteria such as employment and export quantities in order to qualify for private investment incentives;
- Uganda's Investment Code Act stipulates certain screening measures for local and foreign investors intending to invest in information technology.

If the screening mechanism holds the potential to block an investment or M&A in sectors relevant for digital trade, the score is '1'. For a screening mechanism that does not fall in the above category, if two or more mechanisms exist, the score is capped at '0.5'. For any screening mechanisms, the score is '0.25'. If there is no screening mechanism, the score is '0.' Note that anti-trust measures related to M&A are not considered a restriction, unless discriminatory.

Commercial presence requirements

This indicator asks whether an economy imposes any commercial presence requirements to offer cross-border services in sectors relevant to digital trade. Under the **'commercial presence requirement,'** companies must establish their own offices, branches or subsidiaries within the economy to operate the business, for example:

- Indonesia requires all exporters and importers to obtain a permit granted by the Government, which is subjected to a commercial presence requirement;
- Malaysia requires that a foreign company that carries out business in Malaysia to incorporate with a local company or register a branch within the economy;

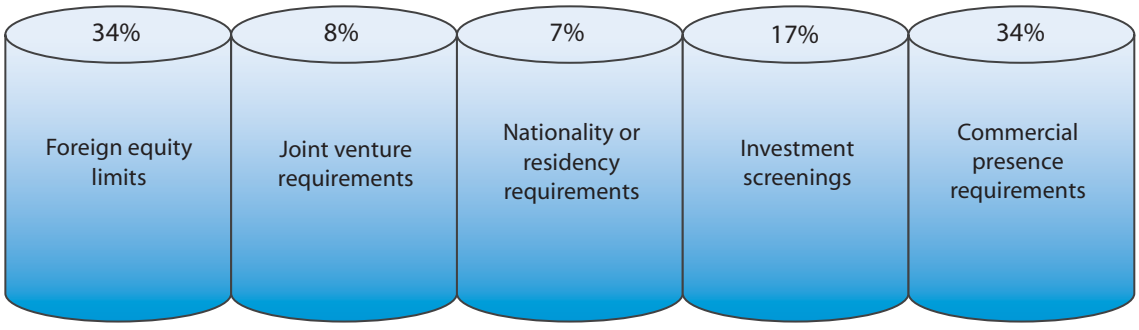
- Colombia's Code of Commerce requires foreign companies to set up a branch in the country to engage in permanent businesses. These include activities such as opening business offices and intervening as a contractor of works or in the provision of services, among others;
- Türkiye requires that online media service providers must obtain a licence for online broadcasting and are required to establish legal entities within the economy;
- Viet Nam requires individuals and organizations operating e-commerce mobile applications must have a branch or representative office within the economy.

For scoring, at least one commercial presence requirement, the score is '1'. Otherwise, the score is '0.'

The weights for each indicator

As shown in figure 10, the weights are 34%, 8%, 7%, 17% and 34%, respectively. The greatest weight, 34%, is given to the first and the fifth indicators – foreign equity limits and commercial presence requirements. Numerical limitations on foreign ownership flatly discriminate against foreign investors and directly block foreign investment. The commercial presence requirements imply that digital trade under Service Trade mode 1 is not feasible. In addition, the requirements incur significant costs of infrastructure establishment and human resources in the recipient country. The fourth indicator – screenings of investment and acquisitions – is given the weight of 17% because they discourage foreign investors due to the time and cost involved in the process. The screening mechanisms could have less certainty and may block investments, thereby receiving higher weight than the joint venture requirements (8%) and nationality or residency requirements for directors or managers (7%). For the second indicator – a joint-venture requirement, which while it discourages foreign investment arguably due to the concern for technology transfer, it does not block foreign investment *per se* as the maximum caps on ownership do. The third indicator – nationality or residency requirements for directors or managers – is given the least weight since the degree to which these requirements discourage foreign investment s is relatively limited.

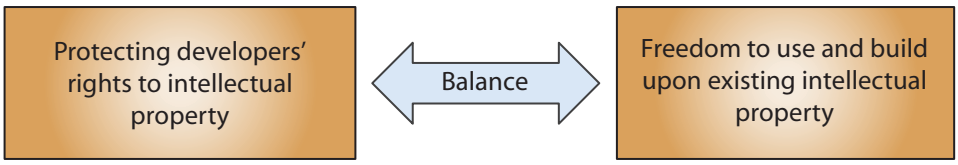
Figure 10 **Pillar 3 indicators and the weights**



Pillar 4. Intellectual property rights

Pillar 4 deals with intellectual property rights (IPRs), which are patents, copyrights and trade secrets. Since sectors relevant to digital trade are knowledge-intensive, IPRs play a crucial role in fostering innovation and creativity in digital trade. Generally, as shown in figure 11, sound policies regarding IPRs find a proper balance between the interests of protecting individual rights to intellectual property and fostering the freedom to use and build upon existing intellectual property. On the other hand, IP policies based on an ill-conceived balance tend to restrict digital trade because they contribute to creating an uncertain regulatory environment.

Figure 11 **Balance in different policy objectives in Pillar 4**



Pillar 4 comprises the following indicators:

- Patent application issues;
- Patent enforcement issues;
- Not in the WIPO Patent Cooperation Treaty (PCT);
- Lack of copyright framework and exceptions;
- Online copyright enforcement issues;
- Not in the WIPO Copyright Treaty (WCT);
- Not in the WIPO Performances and Phonograms Treaty (WPPT);
- Mandatory disclosure of trade secrets; and
- Lack of effective trade secrets legal framework.

Patent application issues

This indicator covers measures on the application process for local and international patents, including differential treatment between local and foreign applications, and the measures applied on both applications. The indicator asks whether there is a restriction on patent application process, and what type of such restriction.

The differential treatment, such as the different terms of patent protection that apply to foreign applicants rather than to domestic applicants discourage or discriminate against foreign applicants. The domestic measures applied to both local and foreign applicant appear in various forms, such as the requirement to appoint a local patent agent, a rejection of the patent application in a discretionary manner, high filing fees, lack of institutional transparency, low quality of substantive examination,[10] high costs for registration and a requirement to file a patent locally before filing aboard.

[10] Substantive examination is a procedure when the authority examines the submitted patent application and determines whether the requested invention meets the patentability requirement, i.e., new and inventive.

For example:

- A rejection of the patent application in a discretionary manner. For example, in the Lao People's Democratic Republic (Lao PDR), a patent or petty patent will be refused if contrary to the culture, social orders and security. With regard to this case, the rejection of patents based on the grounds of public policy is uncertain and burdens the applicants who wish to seek a patent registration in such an economy.
- A requirement to appoint a local agent. For example, Viet Nam requires patent applications by non-Vietnamese residents must be filed via recognized Vietnamese legal representative.
- A requirement to satisfy local requirements before filing abroad. For example, China requires that, where a Chinese entity or individual intends to file a patent application in a foreign economy for an invention made in China, the applicant must submit the matter to request the patent administration department for confidentialily examination in advance. This provision is applicable to all Chinese entities, including a subsidiary of a foreign company which is also considered a Chinese entity. Nepal has also introduced a regime where foreign patents are not valid in Nepal unless they are registered in Nepal.

For scoring, the score is '1' if there exists differential treatment between local and foreign firms, requirements to appoint a local representative and a rejection of patent application in a discriminatory manner. The score is '0.5' for a non-transparent process, high filing fees, high registration costs, substantive examination and the requirement to file a patent locally before filing abroad. The score is '0' if there is no restriction and the patent application process is transparent.

Patent enforcement issues

This indicator covers measures on the enforcement of patents. The indicator asks whether there is a restriction on patent enforcement and the scope of such restriction.

The measures that will get scored may include, for example, different terms of patent protection that discriminate against the enforcement of foreign patent applicants,[11] the patent enforcement is not transparent, lengthy proceedings, and inadequate or non-deterrent sanctions. The scope of the patent enforcement restrictions horizontally applied to all cases and to all sectors, or limitedly applied to a specific circumstance or one sector constitute different impacts on businesses. For example, of the horizontal case, the Russian Federation permits the Government to use inventions, utility models, and industrial designs without consent of the patent holder when justified by the extreme needs of national defense and security or the protection of life or public health. The patent holder must be notified and compensated.

For scoring, the score is '1' when a restriction on patent enforcement is considered to have a high impact. This occurs, for example, when the issue is pervasive affecting all circumstances and sectors, or if there are two or more patent enforcement measures applied to a limited case or a specific sector. The score is '0.5' if a measure is applied to a limited case or a specific sector. The score is '0' if there is no discrimination and patent enforcement is transparent.

[11] Different terms of patent protection that apply to foreign applicants than to domestic applicants would likely mean that the economy does not accord national treatment because it is not a party to the Paris Convention or the WTO, which is very rare or the economy imposes this restriction as an exception to the Paris Convention or TRIPS Agreement.

Not in the WIPO Patent Cooperation Treaty (PCT)

This indicator looks at whether an economy is a member of the WIPO Patent Cooperation Treaty (PCT) (box 3). The PCT is a multilateral treaty and creates a unified patent system, which provides several advantages to residents or nationals of PCT members. The lack of PCT membership can increase the risks of elevated regulatory compliance costs, especially when the businesses wish to establish a patent in other member economies.

The score is '1' if an economy is not a member of the PCT. Otherwise, the score is '0'. To see contracting parties in the Treaty, check the PCT Applicant's Guide (national phase) or the official government website.

Box 3

The Patent Cooperation Treaty (PCT)

The PCT was concluded in 1970, and as of 2023 had more than 150 Contracting States. The PCT facilitates patent protection for an invention simultaneously in many economies consisting of "international" and "national" phases. It begins with the filing of a single "international" patent application. The granting of patents remains under the control of the national or regional patent offices in what is called the "national phase".

The PCT has several advantages. First, an international patent application under the PCT provides the applicant with an international search report and a written opinion on the potential patentability of the patent in the member economies. Although the international patent application alone does not grant a patent unless an application is filed subsequently in a national or regional patent office of the territory where the applicant wishes to establish a patent (or "enters the national phase"): (a) the applicant can refer to these documents to assess the worthiness of filing a patent in national or regional patent offices of the members; and (b) the process of patent prosecution in the national phase becomes easier due to these documents. The applicant may also request a supplementary international search report and international preliminary examination, which is the second evaluation of patentability.

Second, under the PCT, applicants have additional time to decide whether to file in a national or regional patent office to get a patent without worrying that the same invention would get patented in the meantime. This is because the date of filing under the PCT becomes the priority date. The effect of the priority date is that a patent does not become invalidated by reason of any acts by interval such as another filing, publication or sale of the invention. This time could be up to (a) 18 months after an applicant files an international patent application or (b) 30 months after an applicant files with a national or regional patent office of a member economy.

Lack of copyright framework and exceptions

This indicator asks for the presence of a copyright legal framework and what type of copyright exceptions, if any, an economy has adopted. The exceptions allow lawful use of copyrighted works without obtaining permission or a licence from the copyright holders. This encourages foreign persons (natural or legal) to use existing materials copyrighted in an economy and thereby

make innovation and development. However, the degree to which the exceptions promote this interest differs depending on the type of exceptions.

First, the doctrine of fair use provides that if the use of a copyrighted work is fair, the use is lawful. Such use is considered fair in light of several factors such as: (a) the purpose and character of the use; (b) the nature of the copyrighted work; (c) the amount and substantiality of the portion taken; and (d) the effect of the use upon the commercial market. Thus, the doctrine is a flexible, case-by-case test, creating more room for new, innovative use. In general, the use of copyrighted material for criticism, comment, news reporting, teaching, scholarship or research is fair, but not always; furthermore, the use of other than these examples can be fair.

Second, the doctrine of fair dealing provides that the use of copyrighted material is permissible only if the use (a) falls under an exhaustive list of permissible uses, and (b) is fair (e.g., giving proper attribution to the copyright holder). Generally, the list is confined to research, private study, education, satire, parody, criticism, review or news reporting, leaving little 'wriggle room' for subsequent use of copyrighted works.

Last, some economies, such as the Russian Federation and Thailand, have incorporated a test similar to the three-step test. The three-step test was established under Article 9(2) of the Berne Convention for the Protection of Literary and Artistic Works, which states that: "reproduction [of literary and artistic works protected by the Convention] in certain special cases (a) does not conflict with a normal exploitation of the work and (b) does not unreasonably prejudice the legitimate interests of the author." However, this test alone does not say much about what constitutes permissible uses, thus creating uncertainty.

The score is '1' if an economy lacks copyright legal framework or has no copyright exceptions. The score '0.5' is assigned when an economy adopts copyright exceptions but they are not an explicit fair use or fair dealing regime, such as the three-step test and other types of copyright exceptions.[12] The score is '0' if an economy adopts clear copyright exceptions following fair use and/or fair dealing regime.

Online copyright enforcement issues

This indicator asks whether an economy adequately protects copyright against online copyright infringement based on levels of piracy on software and other ICT products in the country. For the purpose of this indicator, the protection is adequate if an economy takes a legislative reform to tackle copyright piracy, if any, and accords national treatment for this protection towards foreign copyright

For scoring, if an economy fails to have a legislative approach to tackle copyright piracy, the score is '1.' If an economy has a legislative framework, there is an issue of discriminatory treatment concerning the protection of copyrights. Therefore, the score is also '1'. If there is no complaint from an established source about copyright piracy, the score is '0.'

[12] For example, Indonesia implements abroad copyright exception for "making and disseminating copyright content through information and communication technology media that is non-commercial and/or non-profit in its effect on the author or related parties, or in which the author has expressed no objection to such making or disseminating". Kazakhstan adopts copyright exceptions similar to fair use or fair dealing. However, these exceptions have a limited scope, such as the exceptions for photographic works, works of fine art permanently located in public spaces, and the broadcasting of architectural works. Moreover, the Russian Federation adopts the concept that "free use" copyright exceptions with limited scope and means (reproduction of articles and audio-visual works) in different new medias is allowed within reporting on "current economic, political, social and religious matters, implying that using any works to report on unrelated topics is not permitted (Sobol M., 2016).

The latest National Trade Estimate and Special 301 Reports by the Office of the U.S. Trade Representative are useful secondary sources. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Not in the WIPO Copyright Treaty

This indicator looks at whether an economy is a signatory to the WIPO Patent Cooperation Treaty (WCT) (box 4). The WCT is a special agreement under the Berne Convention for the Protection of Literary and Artistic Works and ensures the protection of works and the rights of their authors in the digital environment.

The WCT expands the scope of copyright protection to two subject matters for at least 50 years: (a) computer programs, whatever the mode of form of their expression; and (b) compilations of data ("database"), in any form, their contents constitute intellectual creation.[13] The Treaty grants exclusive rights apart from the rights recognized by the Berne Convention to authors, which are the right of distribution, the right of rental and the right of communication by wire or wireless transmission.[14]

The score is '1' if an economy is not a member of the WCT. Otherwise, the score is '0'. To see contracting parties in the Treaty, check the WIPO official site or the official government website.

Not in the WIPO Performances and Phonograms Treaty (WPPT)

This indicator looks at whether an economy is a signatory to the WIPO Performances and Phonograms Treaty (WPPT) (box 4). The WPPT ensures the rights connected to aural performances which are subject matter of phonograms.[15] Two kinds of beneficiaries in the digital environment are focused on: (a) performers (actors, singers, musicians, etc.) and (b) producers of phonograms (person or legal entities that take the initiative and have the responsibility for the fixation of sounds). The term of protection of these rights is 50 years.

The Treaty grants exclusive right to the performances fixed in phonograms (excluding audiovisual fixations, such as motion pictures) and phonograms. The rights are the right of reproduction, the right of distribution, the right of rental and the right of making available by wire or wireless transmission.[16] The performers of the unfixed (live) performances also receive the right of

[13] If a database does not constitute such a creation, it is outside the scope of this Treaty. For more information, available at https://www.wipo.int/treaties/en/ip/wct/summary_wct.html

[14] For the rights granted to authors, (a) the right of distribution is the right to authorize the making the copyright works available to the public through sale or transfer of ownership, (b) the right of rental is the right to authorize commercial rental of the copyright work to the public, and (c) the right of communication to the public is the right to authorize any communication by wire or wireless means, including though the Internet.

[15] According to Article 2(b) of the Treaty, "Phonogram" means the fixation of the sounds of a performance or of other sources, or of a representation of sounds other than in the form of a fixation incorporated in a cinematographic or audiovisual work. Also, under Article 2(c) "Fixation" means the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device.

[16] For the rights granted to authors, (a) the right of distribution is the right to authorize the making the copyright works available to the public through sale or transfer of ownership; (b) the right of rental is the right to authorize commercial rental of the copyright work to the public; and (c) the right of communication to the public is the right to authorize any communication by wire or wireless means, including though the Internet.

broadcasting, the right of communication to the public, the right of fixation as well as the moral right that is the right to claim to be identified as the performer and object to any distortion or modification that would be prejudicial to their reputation.

The score is '1' if an economy is not a member of the WPPT. Otherwise, the score is '0'. To see contracting parties in the Treaty, check the WIPO official site or the official government website.

Box 4

The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)

The WCT and WPPT were known as the "Internet Treaties". Both treaties were concluded in 1996 and entered into force in 2002. As of 2023, both treaties have more than 100 Contracting States. The purpose of the two treaties is to update the existing WIPO Treaties on copyright and related rights in accordance with the development of digital technologies and the dissemination of protected material over digital networks. Thereby, these treaties contain several provisions related to the digital agenda, namely the rights applicable for the storage and transmission of works in digital systems, the exceptions to rights in a digital environment (the three-step test under the Berne Convention), and the technological measures of protection and rights management information.

The contracting parties will adopt the Treaties in accordance with their legal systems and oblige ensurance that their enforcement procedures are available to protect against copyright infringement. Although the exercise of rights may be difficult to apply sufficiently in the online environment or the digital uses of works, the 'technological protection measure' (TPM) and 'the rights management information' (RMI) have been introduced to address such concerns in both Treaties.

The **'obligation concerning technological protection measures'** prescribes that the contracting parties shall provide legal protection and effective legal remedies against unauthorized circumvention of effective technological measures. The TPM protects against circumvention of technologies that control access to copyright works. The circumvention of technologies refers to decrypting an encrypt work, avoiding, bypassing, removing, deactivating, or impacting a technological measure without authorization by the copyright owner. The protection can be components, software or any devices, such as passwords or encryption keys, that are capable of protecting the copyright from being copied or accessed.

The **'obligation concerning rights management information'** prescribes that the parties shall provide adequate and effective legal remedies to a person having reasonable ground to know that they remove or alter electronic right management without authority; or distribute or make the copies of the copyright works available by knowing that electronic rights management has been removed or altered without authority. The RMI protects electronic rights management information against authorized access. The information means the information that identifies the work, the author, the owner of any right or the terms and conditions, and any numbers or codes that represent such information when any of this information is attached to a copy of a work or appears in connection with the communication of a work to the public. This information is necessary for the management of the rights.

Mandatory disclosure of trade secrets

This indicator asks whether a Government imposes a mandatory disclosure of trade secrets such as source code and algorithms. For example:

- In Russian Federation, the Foreign Security Service has the right to access or receive the information systems and/or databases on a gratuitous basis.
- In China, to ensure the security and controllability of the information system, companies could be required to provide source code or encryption keys.
- In Malawi, there are requirements for encryption service providers to declare the means of encryption and the source code of the software used by the Malawi Communications Regulatory Authority.

According to the WTO Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement Article 39(3) (Section 7 protection of undisclosed information), "…The submission of undisclosed test or other data shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use."[17] Hence, the requirement could be of limited scope, meaning that the disclosure is conditional or becomes mandatory only in certain circumstances. For example, an economy may adopt an escrow requirement for source codes in public procurement. Suppliers transfer the source codes to an escrow, and the source codes would be transferred to the Government, for example, when the suppliers go bankrupt or refuse to fix their products or programmes. Indonesia has an escrow requirement for custom-made software.

Following WTO TRIPS Article 39(3), it will not get scored when the Government mandates to disclose trade secrets and protects such information against unfair commercial use. If the Government does not provide safeguards against unfair commercial use, a disclosure requirement of limited scope affecting only specific types of products or specific circumstance (for example, disclosure under the national security threat provision[18] for certain companies) will get a score of 0.5. The score is '1' if there is more than one such measure or if the requirement is affecting an entire sector or all sectors horizontally. If there is no such measure, the score is '0.'

Lack of effective trade secrets legal framework

This indicator asks whether an economy has adopted a trade secrets legal framework that provides effective protection of trade secrets. The establishment of trade secrets law ensures that confidential business information or commercially valuable data are protected from unauthorized acquisition, use or disclosure. The absence of trade secret protection could risk misappropriation and potentially discourage the business from operating within certain economies. The scope of indicator is the protection of trade secrets under domestic laws, i.e., intellectual property law and other laws. All forms of trade secret legal framework, such as an Act, provision or a clause, are taken into consideration.

[17] See https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm

[18] GATS Article XIV bis stipulates Security Exceptions, allowing members the flexibility to implement a measure which is considered necessary for the protection of its essential security interests. However, the absence of clarity in defining and determining national security provisions introduces potential obstacles to digital trade. Due to the challenge of interpreting the ambiguous nature of national security, a score of 0.5 or 1.0 is assigned when a country implements a disclosure requirement based on these objectives, depending on the scope of such measures. For more information about GATS Article XIV.
https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_bis_oth.pdf

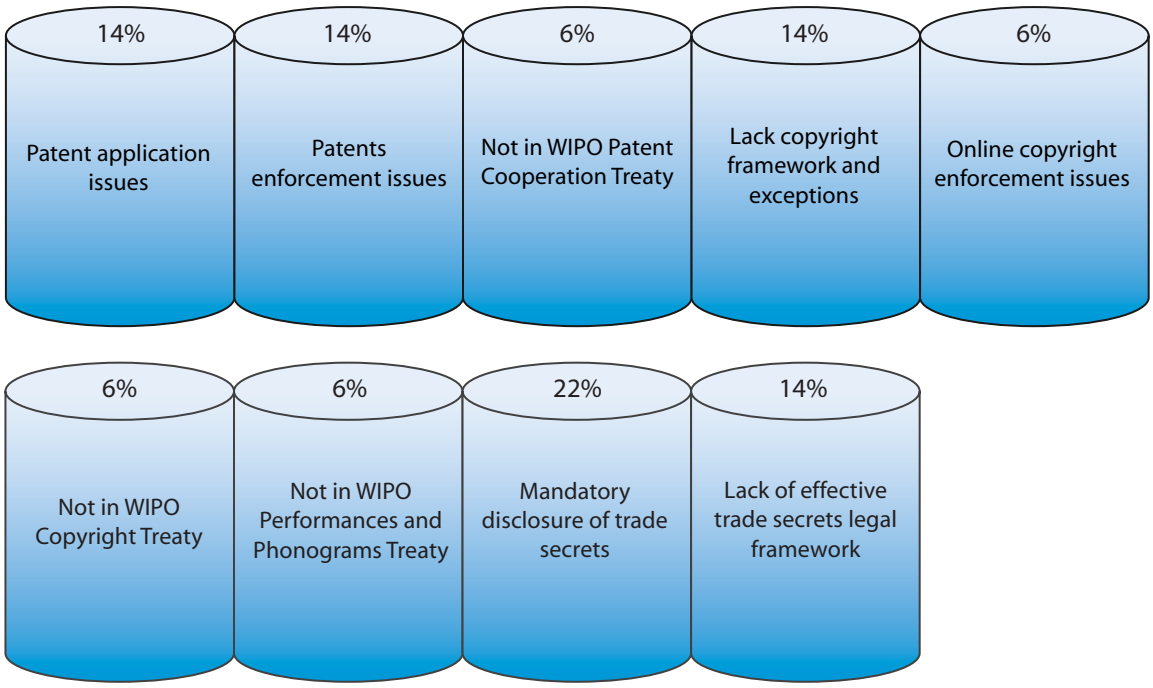
The score is '1' if an economy lacks a trade secrets legal framework that is able to provide effective protection. The score will be 0.5 if it takes in the form of more limited in scope or practices with certain clauses included in the IP law or other relevant law. The score is '0' if there is a presence of a regime for effective trade secrets protection in any forms.

The weights for each indicator

As shown in figure 12, the weight of each intellectual property indicator is given weight of 14%, 14%, 6%, 14%, 6%, 6%, 6%, 22% and 14%. Mandatory disclosure of business trade secrets without taking a proper measure, the eighth indicator receives the highest weight of 22% because the disclosure is against the exclusive right. It could risk unfair commercial use and affect the rights holders' commercial value, thereby competition. The first, second, fourth and nineth indicators with regards to the existence and effective enforcement of patent, copyright and trade secrets are assigned an equal weight of 14% because these indicators do not directly take away the rightsholders' competitive advantage. However, without the transparent patent application process, clear copyright exception and effective patent and trade secrets enforcement could limit innovation and, in some cases, increase infringements.

The remaining indicators captured on the international frameworks and the enforcement of copyright online accounted for the lowest weight of 6% each. The Patent Cooperation Treaty facilitates patent application process. The Copyright Treaty, and the WIPO Performances and Phonograms Treaty strengthen copyright protection in the digital environment. However, not being a signatory of these treaties does not necessarily violate the protected rights. The inadequate enforcement for online copyright partially focuses on online materials, whereas other indicators capture both online and physical subject matters, therefore having a limited impact.

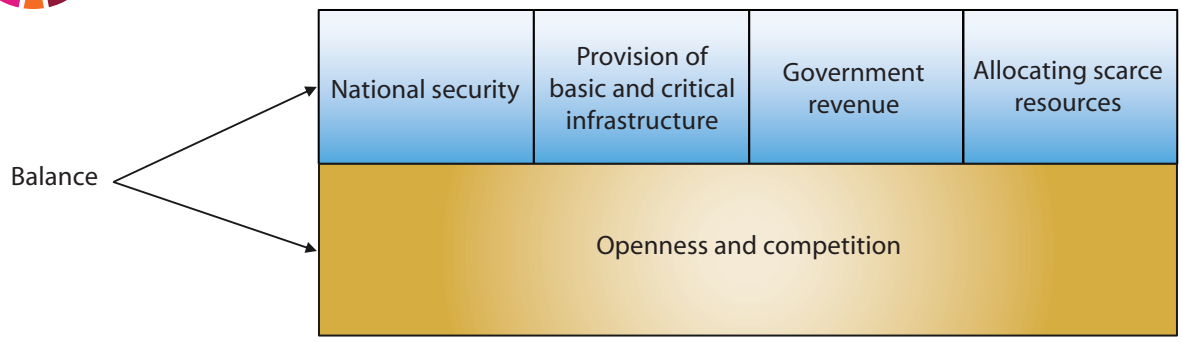
Figure 12 **Pillar 4 indicators and the weights**



Pillar 5. Telecommunications regulations and competition

Pillar 5 deals with policies regarding telecommunications infrastructure and competition. For these policies, relevant policy objectives such as national security, provision of critical infrastructure, raising government revenue and effective allocation of scarce resources invite regulation of the market by the Government. However, for a domestic telecom market to benefit from digital trade, often by means of foreign investment, these policy objectives need to be balanced, as shown in figure 13, with the policy environment that is conducive to competition among domestic and foreign telecom providers.

Figure 13 **Balance in different policy objectives in Pillar 5**



Pillar 5 flags telecom policies and practices that undermine the competition in the telecom sectors by covering:

- Lack of passive infrastructure sharing;
- Foreign equity limits in telecom sector;
- Shares owned by the Government;
- Lack of functional/accounting separation;
- Licensing requirements in telecom sector;
- Not in the WTO Telecom Reference Paper; and
- Lack of independent telecom authority.

Useful secondary sources include the International Comparative Legal Guides (ICLG), Lexology ("Getting the Deal Through"), the National Trade Estimate, Investment Climate Statements by the U.S. Department of State, the OECD Digital STRI database, and the OECD STRI on Telecommunication Services. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Lack of passive infrastructure sharing

This indicator looks at (a) whether there is an obligation for passive infrastructure sharing in the economy, and (b) whether the adopted regulatory approach is mandatory or optional sharing.

'The passive infrastructure' refers to the sharing of non-electronic infrastructure or the physical infrastructure, such as buildings, sites, network cabinet, masts (towers), poles, ducts and trays.[19]

The telecom infrastructure involves high costs, i.e., installation, equipment, operation and maintenance costs. The infrastructure sharing obligation is the process by which one or more telecom operators share infrastructure to deliver services to the end-users. This obligation, thereby, lowers the network deployment, especially in rural areas or marginal markets, stimulates migration to new technologies and the deployment of mobile broadband, and enhances competition between telecom operators and service providers, when safeguards are used to prevent anti-competitive behaviour (ITU, n.d.). Moreover, the infrastructure sharing obligation can be established under various business models and forms.

For example:

- The passive infrastructure sharing obligation is mandated. For example, Thailand requires telecom operators to share their wireless telecommunication network infrastructures with other telecom operators in a reasonable and fair manner, without discrimination. The sharing includes passive infrastructure, namely tower/mast, site, building, HVAC (heating, ventilation and air conditioning) security, and other physical facilities.
- The passive infrastructure sharing obligation is optional but is implemented. For example, Hong Kong, China as well as Pakistan, Singapore and Vanuatu do not mandate passive sharing obligation. However, infrastructure sharing is effective based on commercial agreement in both mobile and fixed sectors. Australia does not require sharing obligation; however, the co-location in the mobile sector is negotiated on a commercial basis. Telecommunication carriers have regulated rights of access to towers owned by other carriers.
- The passive infrastructure obligation is mandated in a specific circumstance, or upon a request. For example, Australia does not mandate passive infrastructure sharing obligation, however, the obligation is in practice in the fixed sector. Once the Australian Competition and Consumer Commission has declared the following services, i.e., line sharing service (LSS), local carriage service (LCS) etc., a network owner must provide access to service upon request.

The score is '1' for the absence of passive infrastructure sharing obligation. The score is '0.5' if the passive sharing obligation is not mandated, but is practiced in the market, or if the obligation is mandated on a case-by-case basis. The score is '0' if the economy mandates at least one obligation for passive infrastructure sharing.

Foreign equity limits in telecom sector

This indicator concerns maximum foreign equity shares in the specific sector of telecommunication, including requirements on shares in government-controlled companies. Foreign equity shares are shares that foreign natural or legal persons hold in a firm incorporated in the investee economy. Foreign investment is a driving force to increase competition and

[19] The infrastructure sharing obligation includes two categories – passive and active infrastructure sharing obligations. The passive infrastructure sharing obligation as mentioned, captures the sharing of physical telecom infrastructure. On the other hand, the active infrastructure sharing obligation captures on active infrastructure of the network (i.e., electronic), including radio access network (antennas, backhaul networks and controllers) and core network (servers and core network functionalities) (GSMA, 2019).

transformation in the telecom market. Limitation on foreign equity shares is a direct obstacle for foreign investors that could induce a higher level of development in the telecom sector. In particular, the foreign equity shares under this Pillar do not include the foreign equity shares in other sectors relevant to digital trade or the e-commerce sector, which are captured in Pillars 3 and 12 respectively.

The score is '1' if there is a ban on foreign ownership in the telecommunication sector or if only a minority stake (less than 50%) is allowed in more than one measure. The score is '0.8' if only a minority stake is allowed. The score is '0.5' where a controlling stake (more than 50%) is allowed, but maximum caps on foreign equity exist or where limitations on foreign equity shares only exist in state-owned enterprises (SOEs). The score is '0' if there is no limitation on foreign equity share in the telecommunication sector.

Shares owned by the Government

This indicator concerns the percentage of shares owned by the Government in telecom companies, including the case in which the telecom operator is an SOE. Most of the government ownership in the telecommunication company limits the local and foreign ownership in the telecom market.

The score is '1' if the Government's ownership in at least one company is above 50%. The score is also '1' if government ownership in more than one company is between 1% and 50%. The score is '0.5' if government ownership in one company is between 1% and 50%. The score is '0' if there no shares owned by the Government in telecom companies.

An example is the Nepal Telecom (NTC) or Nepal Doorsanchar Company Limited (NDCL), the incumbent telecommunications operator in Nepal, which is a state-owned company, with a government share up to 90%. In addition, in Honduras, the Honduran Telecommunications Company (HONDUTEL) is a fully state-owned enterprise.

Lack of functional/accounting separation

This indicator asks whether the economy mandates functional and/or accounting separation for operators with significant market power (SMP) in the telecom market. The SMP refers to the regulatory status representing a dominant position in the telecom market. Functional and accounting separation enhance cost transparency, promote fair market prices, and avoid SMP and non-discriminatory practices in telecom markets.

'Functional separation'[20] refers to the separation of units operating different activity branches in the telecommunication company. The functional separation prevents entities with domain position from controlling operations in another area. For example, Japan requires that NTT EAST/WEST, a Japanese telecom company which owns essential facilities must implement functional separation, such as setting up firewalls between network development and service development.

'Accounting separation' refers to the separation of accounting records for different businesses and parts of businesses run by the same company, so that the costs, revenue and assets associated with each part of a business can be separately identified and properly allocated. This

[20] 'Functional separation' sometimes known as 'operational separation'.

kind of separation ensures that the telecom company accurately reports its financial performance in each area of its operations. For example, Thailand requires a telecom service provider that is determined as having a SMP in the market shall submit the accounting separation annually. Australia mandated a telecom company to maintain separate accounts for its different technology units.

The score is '1' for the absence of separation requirement. The score is '0.5' if only accounting separation. The score is '0.25' when only functional separation is mandated. The score is '0' if the economy mandates both accounting and functional separation of dominant network operators.

Licensing requirements in telecom sector

This indicator refers to a licence for private telecommunication services or to operate telecommunication facilities. It asks (a) whether there are "strict" licensing requirements for telecom-facility providers, network providers and telecom-service providers; and (b) whether there are discriminatory conditions and fees that are applied to foreign companies, minimum capital requirements, and mandatory performance requirements to obtain licences for providing telecom facilities or services.

Regarding the first question, while most economies have licensing schemes in sectors relevant to telecommunications, licensing schemes in certain sectors are "strict", in that they have the potential to block businesses from providing telecom facilities, networks or telecom services. These sectors include services using radio frequencies, broadcasting services and Voice-over-Internet-Protocol services (VoIP). For example:

- Indonesia carries out administrative licensing to allocate radio frequencies rather than holding an auction for the frequencies;
- Ghana requires authorization or a licence issued by the National Media Commission to broadcast content on any public electronic communications network, public electronic communications service or broadcasting service;
- Cambodia, China, the Russian Federation and Singapore require licences for the provision of VoIP services;
- New Zealand and Thailand require licences for the provision of some broadcasting services.

Furthermore, licensing schemes that are well-established practices have some requirements (or conditions) for obtaining a licence that is "strict" in the same sense. For example:

- Nepal imposes a cap on the maximum number of licences for facility providers. No other licences will be issued for five years after the first two licences have been issued for the development of telecommunications infrastructure;
- Tanzania requires holders of licences for network facilities and network services to offer a minimum of 25% of the company's share to the public through an initial public offering on the stock market;
- India imposes a considerable one-time licence fee for "the Unified License" for foreign investment in telecommunication services generally as well as sector-specific licences for wireless and wired connection.

Such a licence scheme counts as '1'. Otherwise, the score is '0'.

Useful secondary sources include the Freedom House's report on Freedom on the Net, the World Map of Encryption and the Lexology ("Getting the Deal Through"). The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Not in the WTO Telecom Reference Paper

This indicator captures whether an economy is a signatory to the WTO's Telecom Reference Paper. The Reference Paper prescribes definitions and principles of the six regulatory frameworks for the basic telecommunication services on competitive safeguards, interconnection, universal services obligation, public availability of licensing criteria, independent regulators, and allocation and use of scarce resources. The regulatory framework is legally binding for those WTO Governments which have committed to it by appending the document, in whole or in part, to their schedules of commitments and is enforceable through the WTO dispute settlement (box 5).

The score is '1' if an economy is not appended to the WTO Telecom Reference Paper. The score is '0' if an economy is fully or partially appended to the WTO Telecom Reference Paper. To see the coverage schedule, check the list of telecommunications commitments and exemptions at the WTO schedule of specific commitments and lists of Article II exemptions, telecommunications commitments and exemptions[21] or the official government website.

Box 5

WTO Telecom Reference Paper

In general, all WTO members are bound to GATS which incorporates an Annex on telecommunications to ensure reasonable access and the use of public telecommunications. The WTO Telecom Reference paper is another key element of telecom disciplines resulting from the post-Uruguay Round Ministerial Decision on negotiations of basic telecommunications. The Reference Paper has the status of international treaty. It introduces the regulatory component that allows WTO members to commit to this framework either wholly or partially by appending the document to their schedules of commitments. The purpose of this regulatory framework is to provide a blueprint considering a set of best practices for telecommunications reform when competition is being introduced in the market.

[21] When an economy does not appear in the 'WTO telecommunications commitments and exemptions' list, it does not always mean that an economy does not append to the WTO Telecom Reference Paper. Please double check at the WTO schedule of specific commitments and lists of Article II exemptions or the official government website.

Lack of independent telecom authority

This indicator shows whether there is an executive authority for the supervision and administration of services in the telecommunications sector that is completely independent from the operator and supplier of the telecommunication services, the Government and other interested persons in the decision-making process and administering of decision.[22] An independent telecom authority is expected to promote fair competition and not be involved in a conflict of interest. The decisions and the procedures used by regulators will be impartial.

The score is '1' for the lack of independent telecom authority. Otherwise, the score is '0'.

The weights for each indicator

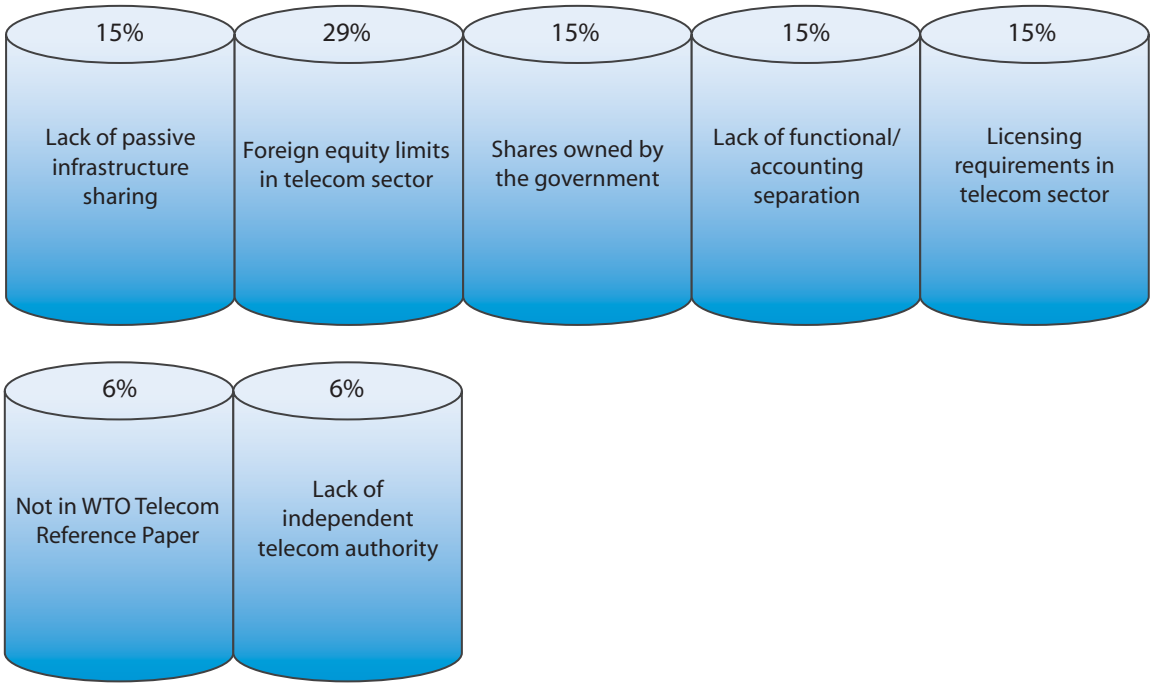
As shown in figure 14, each indicator is given the weight of 15%, 29%, 15%, 15%, 15%, 6% and 6%. The indicators on foreign equity shares and shares owned by Governments reflect the structure of the telecom market in the respective economy, and capture the presence of competition in the telecom market. Other indicators on passive infrastructure sharing obligations, functional/accounting separations, licensing schemes that the WTO Telecom Reference Paper and independent telecom authority provide the extent to which competition is in place in a certain telecom market.

Foreign equity limits, the second indicator, is assigned the highest weight of 29%. Foreign ownership limitations discriminate against foreign investors and preclude foreign investment in the telecom sector. For the third indicator, the higher percentage of shares owned by Governments directly affects the competition in the telecom market. However, it affects local and foreign businesses, thereby receiving a lesser weight of 15%. The lack of passive infrastructure sharing requirements and lack of functional and/or accounting separations, the first and fourth indicators, are assigned a similar weight of 15% because the absence of these measures could hamper the entry of new players in the market and discourage the telecom operators for competing with the established operators. In other words, the lack of measures could provide the operators with the dominant position's ability to involve in anti-competitive practices by increasing their controls over the telecom-related facilitates. The strict licensing requirements, the fifth indicator, potentially block or discourage businesses from participating in the telecom sector, hence receive the score of 15%. Moreover, for the sixth and seventh indicators, the WTO Telecom Reference Paper and independent telecom authority are given the least weight of 6% since the absence of these indicators does not mean that competition does not exist, and the extent to which these measures deter foreign business is somewhat minimal.

[22] The concept of independent telecom authority is embodied in the WTO Telecom Reference Paper (Clause 5 Independent Regulators), the WTO Reference Paper on Services Domestic Regulation 2021 (Section 2, Clause 12 Independence) and the International Telecommunication Union (ITU). In the RDTII 2.0, the scope of independent telecom authority is beyond the WTO Reference Paper for the independence from telecommunication operators; it covers the independence from the Government and other interested parties.

Figure 14

Pillar 5 indicators and the weights



Pillar 6. Cross-border data policies

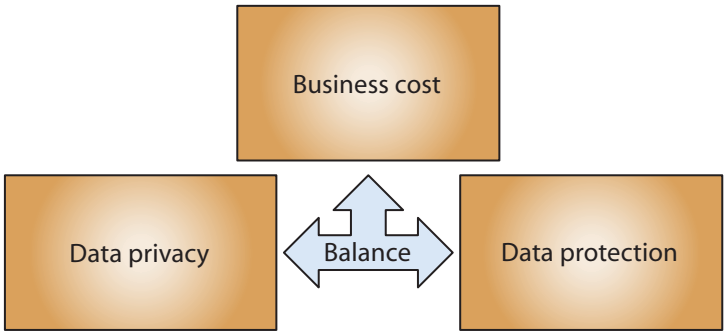
Pillar 6 deals with cross-border data policies by regulating the ways in which data flows from one jurisdiction to another. Important policy considerations are about balancing business costs created by the regulations with the public policy objectives to protect data and data privacy (figure 15).

Regarding business costs, regulation of cross-border data flows tends to increase the cost of compliance as they set up barriers for businesses to store and process data (Ferracane, 2017). Transferring data across borders is a crucial driver of digital trade, as data are integral to the provision of digital goods, online services and even digital-trade infrastructure. Specifically, business models in these areas rely on 'data value chains.' A data value chain, by connecting data acquisition, data storage, data processing and data analysis, offers efficient and smart business solutions for transactions. These transactions occur either within a business or between a business and its customers. Therefore, barriers to the movement of data across borders could heighten the costs for digital trade.

Data privacy and data protection are two sides of the same coin. Data privacy refers to an individual's right to retain control over the way in which their personal data get collected and used, while data protection refers to the responsibility of entities to apply safeguard mechanisms to the handling of data (PECC and Access Partnership, 2021). Without proper data protection, data privacy is threatened; therefore, a high level of data privacy often presupposes strong data protection.

Sound cross-border data policies are often based on a subtle balancing of business costs and digital trust (figure 15). Compliance with data protection rules increases costs. However, the better that data privacy is, and the stronger that cybersecurity is, the greater digital trust the regulatory environment evinces in the eyes of businesses and consumers. This is because there would be fewer data breaches, and, even if there were, stronger accountability mechanisms would exist.

Balance in different policy objectives in Pillar 6



Pillar 6 covers regulatory measures (or lack thereof) on cross-border data transfer that do not get justified in the light of these policy parameters, not necessarily because the measures omit any one of the policy parameters such as business cost, data privacy and cybersecurity, but because the measures fail to find a proper balance of these objectives. The failure to lie in such a balance point makes the measures possibly discourage businesses from engaging in digital trade in the respective regulatory environments.

These regulatory measures (or lack thereof) that Pillar 6 flags tend to be more costly if they apply to personal data rather than non-personal data. **Personal data** refers to any information that relates to an identified or directly or indirectly identifiable individual. Per this definition, personal data are generally (a) sensitive data such as name, surname, email address, identification card, IP address, cookie ID as well as health-related data and data revealing racial or ethnic origin, beliefs and religion, and (b) pseudonymous or 'de-identified' data, i.e., data that make an individual identifiable with additional information. By contrast, **non-personal data** are anonymous data that do not relate to an identified or identifiable individual.

Overregulating personal data flows has a higher opportunity cost than over-regulating non-personal data flows. Personal data are the basis of cross-border online services such as financial, business and IT services. Companies analyse the personal data of their clients to offer the services. Furthermore, personal data creates an opportunity for enterprises to improve their consumer engagement for online services or other types of digital trade (Anant and others, 2020). Personal data, such as location data, websites browsed, searches performed, apps and programs used and Internet usage times, allows companies to understand consumers' needs better. These insights, in turn, help to develop new products and services as well as to personalize advertising and marketing.

This Pillar evaluates the regulatory environment for cross-border data flows through the following indicators:

- Ban and local processing requirements;
- Local storage requirements;
- Infrastructure requirements;
- Conditional flow regimes; and
- Not in an agreement with binding commitments on data transfer.

In this Pillar, the requirements on location of data and data flows generally are found in comprehensive data laws or sectoral laws governing the health sector, financial sector (e.g., credit card information) and telecommunications sector (e.g., computer traffic data), for example. Useful secondary sources include the DTE database, the OECD STRI database, and specialized databases, such as Linklaters, DataGuidance, Lexology and DLA Piper. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Ban and local processing requirements

This indicator asks whether there is a ban on data transfer and local processing requirement. As the business costs arising from a ban and local processing requirement are quite subtle, these requirements are classified under the same indicator (Ferracane, 2017).

'Ban on data transfers' prohibits, *per se*, cross-border transfer of data. **'Local processing requirement'** mandates that businesses process certain data domestically. Processing data refers to various activities involving data, such as collection, organization, structuring, storage, adaptation, use, disclosure and dissemination (European Commission, 2018a). Moreover, to process data locally, foreign companies often need to hire domestic service providers even though the companies may already have their own data processors. This constitutes additional costs for them. The following are examples of local processing requirement:

- Australia requires companies to both store and process health records, excluding personal information within Australia;
- Indonesia requires companies to store and process health data within the economy;
- The Republic of Korea requires financial service providers that use cloud services to locally process credit and unique identification information of their users.

The scoring metrics of this indicator have three features: (a) type of data, a requirement that applies to personal data will get a higher score than a condition that applies to non-personal data; (b) scope of data, a horizontal requirement that applies across sectors will get a higher score than a requirement that applies only to a specific sector (such as financial services or telecommunication sector) or specific data types (such as accounting data and health records); and (c) number of economies, a requirement that applies to a greater number of economies will get a higher scope than a requirement that applies to one economy. A measure applied to the government data should not get scored. The indicator focuses on a measure potentially affecting commercial transactions.

The score is '1' when a ban and/or a local processing requirement covers personal data or applies horizontally across sectors. The score of '1' is also assigned when there are two or more requirements on ban and/or local processing applied to non-personal data, or a specific set of data, or applies to more than one economy. The score is '0.5' when a ban and/or a local processing requirement applies to non-personal data, or a specific set of data, or to one economy. The score is '0' when the data is permitted to be transferred freely without any requirement.

Local storage requirements

This indicator asks whether there is a local storage requirement. **'Local storage requirement'** mandates that a copy of certain data is stored within the economy. Businesses can transfer data across borders as long as a copy of the data is kept within the economy. The following are examples of local storage requirement:

- Australia requires companies to both store and process health records, excluding personal information within Australia;
- Malawi implements a local storage requirement for health-related data;
- New Zealand requires registered entities to store specified tax-related records locally;

- Salvador requires legal entities operating as data information agencies to maintain their databases in the country and to allow access to the superintendence of the financial system; and
- The Russian Federation requires telecom operators to store information about the facts of reception, transmission, delivery and (or) processing of voice information, text messages, images, sounds, video or other messages from users of communication services locally.

Some examples (such as Australia and Brazil), show how some economies impose both local storage and local processing requirements under the same measure. However, the local processing requirements are more demanding than the local storage requirements because the latter requires both processing and storage. This means that a local processing requirement often includes a local storage requirement, while also potentially raising the cost of a foreign firm obliged to locally process the data.

The scoring metrics of this indicator have two features: (a) type of data – a requirement that applies to personal data will get a higher score than a condition that applies to non-personal data; and (b) scope of data – a horizontal requirement that applies across sectors will get a higher score than a requirement that applies only to a specific sector (such as financial services or telecommunication sector) or specific data types (such as accounting data and health records). A measure applied to government data should not get scored. The indicator focuses on a measure potentially affecting commercial transactions.

The score is '1' when a local storage requirement covers personal data or applies horizontally across sectors. The score is '1' and is also assigned when there are two or more local storage requirements applied to non-personal data or a specific set of data. The score is '0.5' when a local storage requirement applies to non-personal data or a specific set of data. The score is '0' when the data are permitted to be transferred freely without any requirement.

Infrastructure requirements

This indicator asks whether there is an infrastructure requirement. **'Infrastructure requirement'** mandates an establishment of a local data centre as a condition to provide certain services using data. The following are examples of infrastructure requirement:

- Kazakhstan requires operators of communications networks to establish a local system of centralized management for their networks;
- Viet Nam requires providers of websites, social networks, mobile network and online games to establish a local server; and
- Chile requires banking institutions outsourcing data processing services outside the country to have a contingency data processing centre located within the country.

The score is '1' when there is at least one infrastructure requirement. The score is '0' when the data are permitted to be transferred freely without any requirement. A measure applied to the government data should not get scored. The indicator focuses on a measure potentially affecting commercial transactions.

Conditional flow regimes

This indicator asks whether an economy adds other conditions for cross-border data transfer. These are another set of conditions that businesses and organizations need to satisfy to transfer data across borders. In other words, even if businesses and organizations satisfy the local storage or processing requirements, they do not get to transfer data unless they also satisfy the set of conditions that this indicator deals with (assuming that the economy imposes these conditions). These conditions prevent businesses and organizations from transferring data to economies where the level of data protection is not adequate or equivalent to the level of domestic data protection.

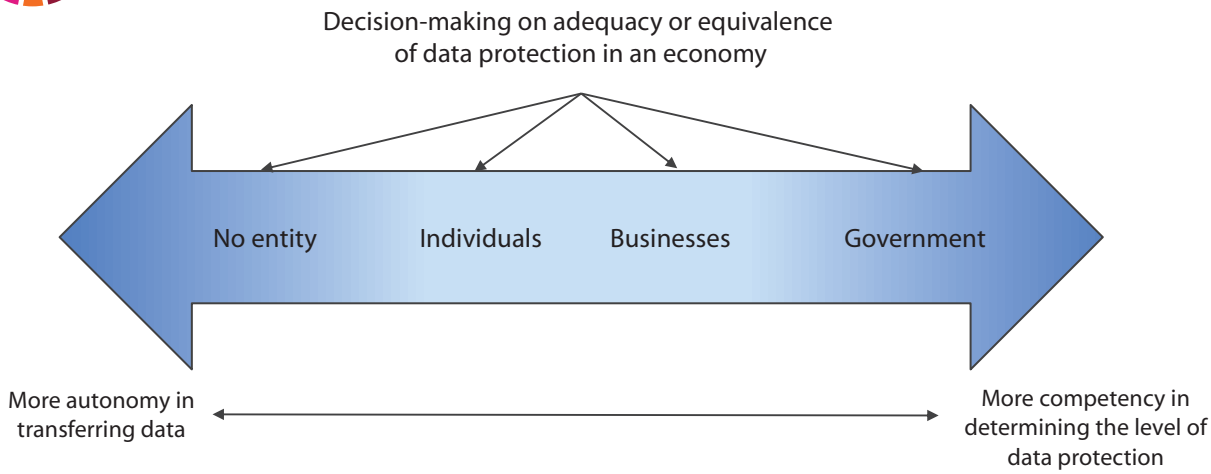
However, the conditions vary depending on which entity decides whether a particular economy has that requisite level of data protection (OECD, 2018). For example:

- There is no condition attached to cross-border data transfer. Thus, naturally, no entity decides the question of the adequacy and equivalence of data protection in economies where data gets transferred. In this case, economies often allow data flows freely across borders, assuming that businesses and organizations that transfer the data are held accountable and liable for possible data breaches that take place in the destination economies;
- Data subjects, who are often individual users, decide whether to allow the transfer of their data to a particular economy by providing their consent;
- Businesses and organizations decide it by evaluating whether a particular economy to which data are about to be transferred has an adequate or equivalent level of data protection;
- The Government determines that certain economies have that requisite level of data protection.

To determine which one of these conditions is more costly than the other is difficult. On the one hand, the lack of such a condition, the consent mechanism, and the mechanism for businesses and organizations' evaluation on this spectrum of the conditions, as shown in figure 16, seem to restrict the movement of data less than the mechanism for the Government's approval. This is either because the movement of data lies in the autonomy of individuals (i.e., data subjects) or because the decision-making is reserved for businesses and organizations rather than the Government. On the other hand, individual users or even businesses may not be competent entities for determining which economy has an adequate or equivalent level of data protection; rather, it is the Government that is in a better position to determine that question, i.e., which economy has an adequate level of data protection.

Figure 16

Conditions of consent, evaluation and approval



The following are examples of these conditions:

- The Russian Federation requires that personal data can be transferred abroad without having additional consent from the data subject. The data must be transferred to the countries that are the parties to the Council of Europe's Convention for the Protection of Individuals and other countries approved by the Russian Federation Service for Supervision of Telecom, Information Technologies and Mass Media (Roskomnadzor);
- Singapore transfer of personal data abroad requires compliance with the Personal Data Protection Act (PDPA) obligations. The recipients outside the country must obtain individual consent to transfer the data and provide a comparable standard of personal data protection as provided in the PDPA;
- Brazil sets out regulations on how financial institutions and other institutions regulated by the Brazilian Central Bank should hire cloud computing services from providers that store or process information outside Brazil. In the absence of a formal agreement with the regulators of the economy where the services are performed, prior authorization is required at least 60 days in advance;
- Türkiye transfers of customer data in the financial sector abroad or to the third parties within the country requires explicit consent from the customer;
- The Republic of Korea transfers of geographical data related to maps or photos produced for the purpose of a survey abroad requires the permission of the Minister of Land, Infrastructure and Transport.

Accordingly, this indicator differentiates the conditions, not based on types of decision-making entities, but based on the two features: (a) type of data, a requirement that applies to personal data, will get a higher score than a condition that applies to non-personal data; and (b) scope of data, a horizontal requirement that applies across sectors will get a higher score than a requirement that applies only to a specific sector (such as financial services or telecommunication sector) or specific data types (such as accounting data and health records). Therefore, the score is '1' if the regime covers personal data or applies horizontally across sectors.

The score is '0.5' when a conditional flow regime applies to non-personal data or a specific set of data (e.g., financial, telecommunications, cloud services etc.). The score is '0' when there is no condition. Moreover, government data are not listed because the database captures the commercial activities.

Not in an agreement with binding commitments on data transfer

This indicator asks whether an economy has committed itself to agreements with a binding commitment on transferring data across borders. The agreement with binding commitment captures all forms (preferential trade agreements or other interoperability initiatives, such as treaties and regional agreements) and types (bilateral, plurilateral, or multinational). The binding provision is enforceable and obliges the party to comply with the agreed provisions. Participating in binding agreements or initiatives safeguards the flow of data and lowers compliance costs.

As for trade agreements, the cross-border data flows provision generally focuses on the commitments to transfer information, including personal information, by electronic means. The data flows provision can be found under various denominations, for example 'Cross-Border Transfer of Information by Electronic Means', 'Cross-Border Information Flows', 'Movement of Information' and 'Free Flow of Data'.

For scoring, the score is '1' if an economy does not commit to any agreements with a binding commitment on cross-border data transfer. The score is '0' if an economy signs at least one binding agreement on data flows. In case the data flows provision or treaty contains both binding and non-binding obligations (considered mixed legalization) such provision will not be scored.[23]

For this indicator, trade agreements, treaties and other commitments are the primary sources, such as official text of the agreements. The Trade Agreements Provisions on Electronic-commerce and Data (TAPED) dataset 2.2.1 [data_free-flow_prov] is a useful secondary source. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

The weights for each indicator

As shown in figure 17, the weight of each indicator varies with regard to cross-border data flows at 38%, 12%, 31%, 12% and 8%, respectively. The first and the third indicators – ban and local processing requirement, as well as infrastructure requirement – are regarded as more weight than the other indicators, at 38% and 31%. A ban on data transfer is costly, in that data are a crucial driver for digital trade. This requirement prohibits data flows, while the rest of the data requirements and conditions permit the data to transfer freely once they have been fulfilled. Local processing requirements relate to several data activities, and businesses may feel a need to build local servers or hire domestic service providers, even though these are not mandatory. Under infrastructure requirement, the businesses are bound to establish data centres or local servers within the economy, increasing fixed costs. Although the requirements to process or to build an

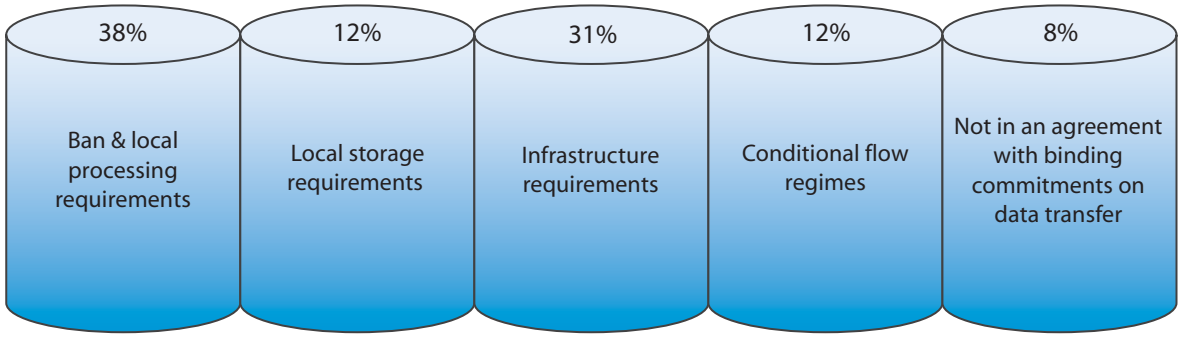
[23] The extent of legalization, i.e., soft legalization (non-binding obligation), mixed legalization (binding and non-binding obligation) and hard legalization (binding obligation), see Codebook TAPED November 2023 version, available at https://www.unilu.ch/fileadmin/fakultaeten/rf/burri/TAPED/Codebook_TAPED_Burri_Vasquez_Kugler_November_2023.pdf

infrastructure for data tend to incur a higher cost of compliance, the processing requirement could create a higher cost as it involves more activities.

Local storage requirements and conditions for cross-border data receive an equal weight of 12%. Local storage has a lesser compliance cost because merely a copy of the data is required to locate within the territory. Still, the requirement may not necessarily promote digital trust because the local storage does not address how data subjects' data is to be actually used aboard. The condition on data flows, while it incurs costs against businesses, it has a rational relationship with ensuring digital trust in regulatory environments where data are to be used, although tangential. For example, the condition that data cannot be transferred unless data protection in receiving economies is deemed adequate tends to ensure that data gets some protection there. However, since the regulating economy has no or little control over data privacy and protection, the effect of such a condition on forming a digital trust may be limited.

In addition, the last indicator, participation to agreement with binding commitment on cross-border data flows, has the least weight (8%). Committing to a binding agreement could help in shaping harmonize data flows regulation and practice across regions. However, not being a member to data flows commitment does not impede the flows of data across borders.

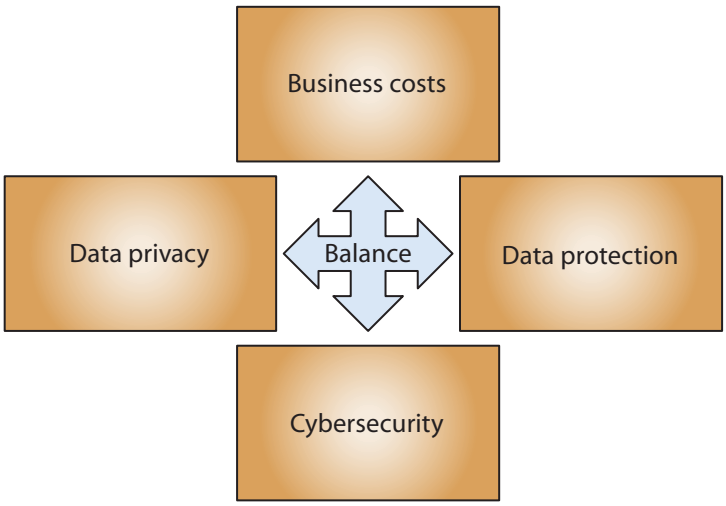
Figure 17 **Pillar 6 indicators and the weights**



Pillar 7. Domestic data protection and privacy

Pillar 7 deals with policies governing the use of data in the regulating economy. In addition to the three policy parameters – business cost, data privacy and data protection – this pilar also focuses on cybersecurity (figure 18). Cybersecurity refers to a Government's enforcement efforts to protect organizations, individuals and networks, both in the public and private sectors, from digital attacks such as "the unauthorized access, modification and extraction of data, the theft of proprietary information and the purposeful incapacitation of critical infrastructure, depending on the scale and intention of the attack in question" (PECC and Access Partnership, 2021). Along with data privacy and data protection, cybersecurity has a significant impact on digital trust.

Figure 18 **Balance in different policy objectives in Pillar 7**



This Pillar considers the following conditions as potentially creating high costs:

- Lack of comprehensive legal framework for data protection;
- Minimum period of data retention requirements;
- Data Protection Impact Assessment (DPIA) or Data Protection Officer (DPO) requirements;
- Requirements to allow government access to personal data.

Useful secondary sources include the UNCTAD Cyberlaw Tracker, Linklaters, DataGuidance, ICLG, Lexology and DLA Piper. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Lack of comprehensive legal framework for data protection

This indicator asks whether an economy has adopted a comprehensive data protection legal framework that applies to personal data across sectors. The significance of data privacy protection lies in its contribution to digital trust and assurance of legal certainty. In this regard, the lack of

data protection laws will create risks for the data subject and poses challenges for businesses. Specifically, the absence of the data legal framework could discourage digital trade because the data users become hesitant to entrust their data with businesses on how their rights will be enforced and the willingness to transfer them to other economies. Businesses and organizations can be held liable for the consequences of data breaches.

The criteria for a "comprehensive" data protection legal framework are that the regulation applies horizontally and includes detailed provisions on the scope and application of rights and obligations of data owner. The comprehensive data protection legal framework empowers individual to control over their personal data, such as the right to access, rectification, erasure, and data portability, and encompasses various activities, such as data collection, data processing and the transfer of personal data across borders.

Compounding this problem is the fragmentation of data protection requirement across sectors. Sectoral data protection obligations such as in finance, health and education can be inter-operated (PECC and Access Partnership, 2021). Often, several sectors are entwined with each other. As seen in the rise of FinTech, data privacy threats to communications and IT sectors also constitute threats to the finance sector. The education, health and e-commerce sectors are dependent on the payments sector, which is, in some jurisdictions, categorized also as a financial entity. Thus, the asymmetry of information from different data privacy and data protection requirements across sectors may add compliance cost to businesses as they navigate through the complexities of regulations.

In this context, regional agreements encourage establishing personal data protection legal frameworks and ensures data privacy protection while facilitating the free flow of data. This facilitation often includes mutual recognition of agreement partners data protection certifications or data protection trustmarks [24] as a mechanism to transfer data.[25]

Accordingly, the scoring metrics for this indicator consider that if an economy lacks this data protection framework, the score is '1'. The score is '0.5' when there is a data protection framework that applies only to specific sectors ('sectoral law'). The score is '0' if there is a comprehensive data protection legal framework.

[24] Data protection trustmarks is a voluntary certification for organizations to demonstrate accountable data protection practices following the international frameworks, such as European Union's General Data Protection Regulation (GDPR) and the APEC Privacy Framework. These trustmarks promote competitive advantage from business and build trust for consumers (Singapore, 2020; Singapore, 2024).

[25] Specifically, CPTPP Article 14.8, and DEPA Article 4.2 states that "to this end, each Party shall adopt or maintain a legal framework that provides protection of the personal information of the users of electronic commerce and digital trade…Each Party shall endevaour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdictions." Notably, DEPA further emphasizes the interconnectedness between data protection and the free flow of data: "The Parties shall endeavour to mutually recognize the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information." Similarly, the African Union Convention on Cyber Security and Personal Data Protection Article 8.1 states that "Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data."

Minimum period of data retention requirements

This indicator asks whether an economy imposes a minimum period of data retention requirements. The data retention requirements regulate how long a company should keep a copy of certain data in order and make it available upon request by the authorities.[26]

The purpose behind these requirements is often to help investigations on certain matters such as corporate affairs and tax payments or to reinforce the Government's law enforcement efforts, especially with regard to communication data from telecom companies.

However, these requirements are not considered to be balanced in terms of the important policy objectives for digital trade – namely, business cost, data privacy and cybersecurity. The data retention requirements increase compliance burdens on businesses. In particular, MSMEs often lack resources to manage data they keep for a substantial period of time per divergent regulatory obligations across economies. The availability of data retained for the purposes of various regulatory investigations might create the false impression that data retention is necessary. The mere convenience of data retention does not necessarily make it necessary.

The requirements also undercut data privacy by requiring companies to store personal data for a set period, even longer than necessary. In some cases, the data retention schemes have become a government tool for accessing personal data (Rucz and Kloosterboer, 2020). Last, the data retention requirements ironically and potentially weaken cybersecurity and digital trust, because data retention practices increase data security risks including data leaks, abuses and misuses. For example, potential unauthorized disclosure of, or access to, retained telecommunications data endangers users' privacy. Hence, users may also be reluctant to engage with companies that will store their data for long periods, except in the case of certain types of data for which a long retention period is necessary, such as medical records.

Data retention requirements can set out a **'minimum period of retention'**.[27] Under the 'minimum period of retention,' firms must retain data at least for a specific period. The prescribed period can be days, months or years, typically from two months to more than 10 years.[28] For example:

- In Malawi, there is a required data retention period of at least 7 years;
- In Australia, a telecommunication service provider is required to keep specific telecommunications data related to the services it offers for two years at least. The data include the subscriber and the accounts of telecommunications devices, the source of communication, the destination of a communication, the date, time and duration of communication, the type of communication, and the location of equipment or a line used;

[26] Data retention requirements differ from local storage requirements in Pillar 6. The retention requirements focus on 'duration', while the latter focus on 'location'. For the data retention requirements, firms can retain data at any location, even abroad, whereas for local storage requirements data must be stored locally. Notably, the data retention and local storage requirements are often found in different laws of a given economy.

[27] There are two types of data retention requirements, 'minimum period of retention' and 'maximum period of retention'. The maximum period of retention is when firms cannot retain data longer than necessary without specifying a period. Businesses have latitude under this type of requirement in determining whether to retain data, because the limitations on the period during which businesses can draw value from personal data could consider as costly. However, without a clear period of retention requirement under the maximum period, it is not scored in the RDTII version 2.0.

[28] A somewhat atypical example of a minimum period of retention is a 'permanent period of retention.' For example, India requires the listing companies to permanently preserve the documents that are listed under Schedule I of the Securities and Exchange Board of India Regulations, such as incorporation documents, share certificates, register of minutes of board meetings and register of members.

- In Mexico, telecommunications concessionaires must keep the data of their users for at least 12 months in a system, and after this period the data must be kept for an extra 12 months in an electronic storage system;
- In Peru, concessionaires must keep specific telecommunications data related to the services provided for a period of 12 months in a computer system, and after this the said data for an additional period of 24 months in an electronic storage system;
- In Botswana, the Financial Intelligence Act requires that information obtained from the customers through customer due diligence, account files and correspondence should be retained for 20 years from the date the transaction was concluded and after the termination of the business relationship;
- In Botswana, Electronic Payments Services Regulations mandate that information should be retained for at least five years from the date that the transaction was concluded and after the termination of the business relationship.

The score is '1' when the minimum period of data retention requirement. The score is '0' when there is no requirement or the requirement of data retention exists but without a specified period. Moreover, government data is not listed because the database captures the commercial activities.

Data Protection Impact Assessment or Data Protection Officer requirements

This indicator asks whether an economy requires firms to appoint a Data Protection Officer (DPO) or perform a Data Protection Impact Assessment (DPIA). The DPOs ensure that a company processes personal data in compliance with data protection rules. The DPIA is a process of identifying risks of data processing operations on users' rights.[29] For example:

- Singapore requires companies to appoint one or more data protection officers to ensure the organization's compliance with the Personal Data Protection Act;
- Türkiye requires companies to appoint "a data controller" who will be responsible for compliance under the Protection of Personal Data Law. If a data controller is located in Türkiye, a contact person for the data controller must be appointed. However, if a data controller is located outside Türkiye a national representative, either a natural or juristic person, must be appointed;
- In Colombia, data controllers and processors must appoint a person, or division within the company, to assume responsibility for the protection of personal data, and in charge of reviewing and solving claims made by data subjects;
- Ghana's Data Protection Act requires data controllers to appoint a data protection officer, also defined as a data protection supervisor, whose role is to monitor the data controller's compliance with the provisions of the Act.

While the purpose of these requirements is to ensure the data privacy of individual users and reinforce data protection, the measures may be costly. Firms, especially MSMEs, may struggle to hire a DPO with expertise in compliance with data laws across economies. Compounding this is that, unlike the European Union's General Data Protection Regulation (GDPR), data

[29] Notably, the GDPR mandates the DPIA to data processing activities "likely to result in a high risk." In the GDPR jurisdictions, the DPIA is commonly applied to the processing of sensitive data on a large scale, and a systematic and extensive personal aspect of an individual, including profiling (European Commission, 2018b).

protection laws in developing economies often fragment. It is difficult for a DPO, even if appointed, to navigate through divergent data protection laws. A less costly alternative could be to make the appointment voluntary as an option to show companies' data privacy policies and practices.

Accordingly, the score is '1' is assigned if there is a requirement for the appointment of a DPO or the application of both DPO and DPIA horizontally across all sectors. The score is '0.5' if the requirements for having DPO or having both DPO and DPIA are applied only to a specific sector. The score is '0' when there is no requirement. Note that the requirement to perform the DPIA is generally introduced following the DPO appointment to ensure compliance with data protection rules. Hence, the scoring metric focuses more on the presence of the DPO requirement.

Requirements to allow government access to personal data

The indicator asks whether the Government can access personal data without a court decision, a judicial warrant or similar legal action. The lack of judicial oversight of this discretionary power could violate fundamental rights and thereby minimize trust in the digital environment. Government interference in one user's data may also create exploitable vulnerabilities in other accounts, such as:

- Authorization by Pakistan for law enforcement agents to access personal data without a court warrant if it is believed that it is "reasonably required" for a criminal investigation;
- In Cuba, although exceptionally, the criminal investigator may use electronic surveillance as an investigative technique without the authorization of the Attorney General of the Republic;
- India requires ISPs to maintain a log of all users connected to their services. The ISPs must provide a complete list of subscribers with password-controlled access to the authorized intelligence agencies at any time.

If this requirement applies, the score is '1'. The score is '0' when there is no requirement.

For this indicator, the World map of encryption laws and policies is also a useful secondary source. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

The weights for each indicator

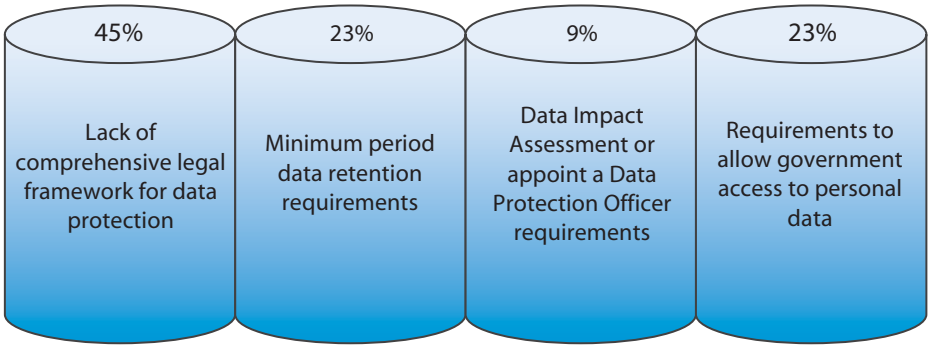
As shown in figure 19, the weights for each indicator are 45%, 23%, 9% and 23%. A lack of comprehensive data protection legal framework that applies across all sectors is given the greatest weight of 45% because having such a legal mechanism is crucial to promoting digital trust. It ensures users' data privacy and appurtenant rights and provides data protection mechanisms. Conversely, the fragmentation of data protection obligations that differ from sector to sector increases regulatory burdens on businesses.

The existence of minimum period of data retention requirements and government access to personal data are given the second greatest weight of 23% because both measures affect digital trust and discourage businesses. Although the second and the fourth indicators increase

compliance cost and undermine data privacy, they are just one cybersecurity mechanism, whereas a comprehensive data protection law contains a bundle of users' rights and data protection mechanisms. Thus its impact is more prevalent. In addition, the data retention requirements incur *ex ante* obligation on the part of businesses and create additional burdens. The Government's access to personal data for law enforcement purposes undercuts digital trust in the eyes of individual users.

The third indicator regarding the requirement to conduct DPIA or appoint a DPO is given the least weight (9%). This is because such a requirement negatively affects only one policy parameter – the cost of compliance; however, it still reinforces data privacy and data protection. The cost that it incurs, especially against MSMEs, does not justify the binding nature of the requirements.

Figure 19 **Pillar 7 indicators and the weights**

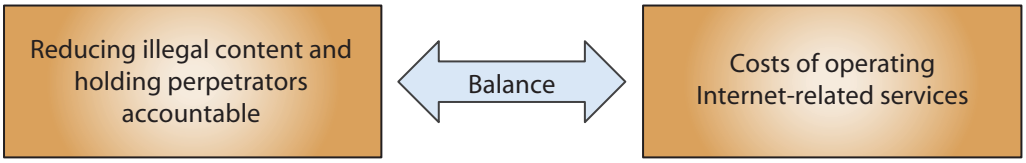


Pillar 8. Internet intermediary liability

Pillar 8 deals with measures governing intermediary liability. **'Internet intermediaries'** can be defined as "the intermediaries that bring together or facilitate transactions between the third parties on the Internet.[30] They give access, transmit and index content, or provide Internet-based services to third parties." In this regard, they facilitate digital trade. The intermediaries include Internet service providers (ISPs) and Internet content providers (ICPs).[31]

Often, the regulation of Internet intermediaries is based on the interest of reducing illegal content over the Internet and holding perpetrators accountable. However, imposing onerous liability or certain obligations on the Internet intermediaries would likely discourage them from participating in digital trade in the regulating economy. Pillar 8 deals with regulatory measures that stand on an ill-placed balance of these two competing objectives, as shown in figure 20.

Figure 20 **Balance in different policy objectives in Pillar 8**



With the balance between these policy objectives, Pillar 8 consists of the following indicators:

- Lack of safe harbour for copyright infringements;
- Lack of safe harbour for other illegal activities;
- User identify requirements; and
- Monitoring requirements.

Useful secondary sources for this Pillar include the DTE database, the reports by the Global Network Initiative, the World Intermediary Liability Map and the NTE reports. The secondary sources should only serve to guide researchers to the primary sources.

Lack of safe harbour for copyright infringements

This indicator asks whether an economy has a safe harbour provision for copyright infringement. A safe harbour provision protects the Internet intermediaries from legal liability for certain activities performed by their users. Without this provision, the Internet intermediaries hosting content in violation of copyrights will be, *per se,* legally responsible for their users' activities even when the intermediaries do not notice it. This may discourage investment in digital platforms. Furthermore,

[30] There is no agreed definition of intermediaries. For more information, see the Oxford Handbook of Online Intermediary Liability (Frosio, 2020); see also OECD, 2011.

[31] Similarly, there is no agreed definition for ISPs and Internet content providers ICPs. ISPs can be defined as entities that provide Internet access and associated services such as email service, browser service, domain name registration and web hosting. There are several types of ISPs – for example, dial-up, cable (broadband), DSL (digital line subscribers) and fibre optics (satellite). ICPs can be defined as entities that disseminate online content to the end-users, such as social media platforms and news providers.

the safe harbour regime supports the emergence of innovative services as it provides intermediaries with legal certainty to conduct a wide range of activities, with less threat of potential liability and the less chilling effect of potential litigation.

This provision that protects the intermediaries from legal liability for copyright-infringing materials can take various forms:

- The intermediaries are protected from legal liability for copyright-infringing materials in their platforms, and illegal activities are forbidden by different laws unless the intermediaries contributed to them or had notice of them beforehand. For example, New Zealand's Copyright (New Technologies) Amendment Act protects ISPs from copyright infringing content created by their users, if they do not have specific knowledge of the infringement or immediately make such content unavailable upon notice. New Zealand's Harmful Digital Communication Act provides protection to an online content host for illegal content posted by its users;
- The intermediaries are protected from legal liability for copyright-infringing materials in their platforms as well as illegal activities under the same law. For example, Japan's Act No.137 of 2001 protects ISPs from liability for damages caused by failing to delete infringing content. The ISPs also protect from any damages caused by the deletion of content on their networks if they reasonably believe that the content infringes intellectual property or privacy of others, or if they sent a notice to the users of such content and have not received a response within seven days; and
- The intermediaries are protected from legal liability for copyright- infringing activities but not for illegal activities. For example, Malaysia's Copyright Amendments Act protects ISPs and ICPs from copyright infringement if they remove or disable access to the infringing content. Still, there is no safe harbour regime for other activities apart from copyright infringement.

The score is '1' for lack of a safe harbour provision for copyright infringement. The score is '0' for a safe harbour provision that protects them from liability for copyright-infringing activities.

Lack of safe harbour for other illegal activities

This indicator asks whether an economy has a safe harbour provision for other illegal activities other than copyright infringement. As mentioned, a safe harbour provision protects the Internet intermediaries from legal liability for certain activities performed by their users. Without this provision, Internet intermediaries hosting illegal content other than copyright infringement will be, *per se,* legally responsible for their users' activities even when the intermediaries do not notice of it. This may discourage investment in digital platforms. Furthermore, the safe harbour regime supports the emergence of innovative services as it provides intermediaries with legal certainty to conduct a wide range of activities, with less threat of potential liability and the less chilling effect of potential litigation.

The provision that protects the intermediaries from legal liability for activities apart from the copyright-infringing materials can take various forms:

- The intermediaries are protected from legal liability for copyright-infringing materials in their platforms, and illegal activities are forbidden by different laws unless the

intermediaries contributed to them or had notice of them beforehand. For example, New Zealand's Copyright (New Technologies) Amendment Act protects ISPs from copyright infringing content created by their users, if they do not have specific knowledge of the infringement or have immediately made such content unavailable upon notice. New Zealand's Harmful Digital Communication Act provides protection to an online content host for illegal content posted by its users; and

- The intermediaries are protected from legal liability for copyright-infringing materials in their platforms, and from illegal activities under the same law. For example, Japan's Act No.137 of 2001 protects ISPs from liability for damages caused by failing to delete infringing content. The ISPs also provide protection from any damages caused by the deletion of content on their networks if they reasonably believe that the content infringes intellectual property or privacy of others, or if they sent a notice to the users of such content and have not received a response within seven days.

The score is '1' for lack of a safe-harbour provision for activities other than copyright infringement. The score is '0' for a safe harbour provision that protects them from liability for illegal activities other than copyright-infringing.

User identity requirements

The indicator asks whether an economy imposes user identity requirements. The **'user identity requirement'** mandates that Internet intermediaries require their users to supply accurate personal information to use their services or networks. This measure can be costly in that the intermediaries are obliged to act as "gatekeepers" of the Internet, policing their users on behalf of the Government. This requires substantial efforts for the intermediaries to ensure that their users supply accurate personal information. For example:

- Rwanda requires electronic communications service providers to ensure that their users supply accurate personal information when using a service or a network according to the Law Governing Information Communication and Technologies;
- Uganda's Regulation of Interception of Communications Act requires intermediaries to collect customer information (name, address, identification number), install surveillance equipment and disclose information to the authorities upon the presentation of a warrant or a demand from the Minister for Information and Communications Technology and National Guidance;
- Cambodia requires mobile operators to register the identities of their consumers. SIM card dealers are asked to make copies of clients' national identity card, passports or other valid identity document before activating the SIM cards;
- Argentina states that mobile communications service providers must store and systematize information of the user in a registry of owner users of mobile communication service. Information that has to be provided includes the name, surname, national identity document and address of users;
- In Venezuela, operators that provide mobile telephony services (prepaid or post-paid) must require their subscribers to provide personal information when contracting the referred service – for instance, their personal identification number, address, signature and fingerprints;

- Singapore requires mobile service providers to record the personal details of their customers who buy prepaid SIM cards.

The score is '1' if there is user identity requirement and is implemented in order to connect to the Internet or access to online services. The score is '0.5' if user identity requirement is implemented for Subscriber Identity Module (SIM) card registration. Otherwise, the score is '0'.

Monitoring requirements

The entry asks whether an economy imposes content monitoring requirements. The **'monitoring requirement'** mandates that Internet intermediaries to monitor the users' activities or remove or block content that is deemed illegal to avoid legal liability due to such content. Similar to the user identity requirement, intermediaries are obliged to act as "gatekeepers" of the Internet, policing their content on behalf of the Government. This measure requires substantial efforts for the intermediaries to monitor anything that is posted, shared or transferred by the users through the platform, and thereby could incur the cost. For example:

- Lao PDR requires ISPs to monitor the information disseminated through their services to censor criticism against the Government and other political content. The website owners or website managers should also check their content thoroughly before allowing others to disseminate the content through their websites;
- Kazakhstan requires ISPs to monitor content in their networks and hold the responsibility to restrict online material, otherwise they will be subjected to fines for not complying with censorship orders.
- The Nepal Telecommunications Authority (NTA) has made it mandatory for ISPs to install filtering software to block websites that are considered "obscene, seductive and corrupt social morals" or that threaten "religious harmony, national security, and go against values and beliefs of the state.

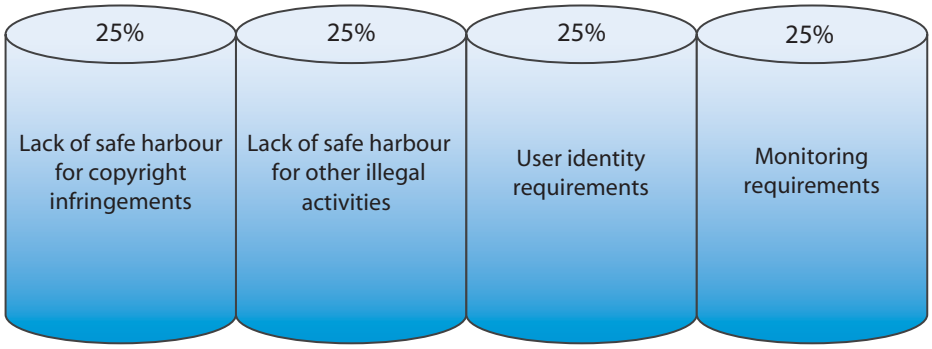
The score is '1' if at least one monitoring requirement is implemented. The score 0.5 for the requirement of active monitoring of users' activities without any legal obligation to remove or block the content. Otherwise, the score is '0'.

The weights for each indicator

As shown in figure 21, an equal weight of 25% is given because each indicator seems to be an equally important requirement for Internet intermediaries. Regarding the first and second indicators, without the safe harbour provision in place, the intermediaries face a higher risk of being liable for their users' activities and the costs of litigation. The third and fourth indicators on user identity and monitoring requirements imposes on the intermediaries' additional responsibilities and thus incur costs. The intermediaries must procure additional software or hire an additional workforce to monitor online activities and collect their users' identities. In addition, to mitigate the liability arising from their users' activity due to the lack of safe harbour and the existing monitoring requirements, the intermediaries may impose unnecessary blocking and filtering, which are the measures under Pillar 9.

Figure 21

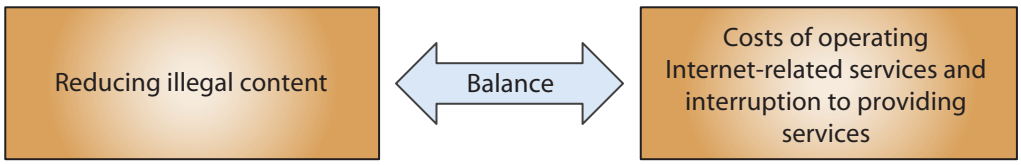
Pillar 8 indicators and the weights



Pillar 9. Content access

Pillar 9 deals with requirements on content access, which is somewhat connected to Pillar 8, Internet intermediary liabilities. Regulations of content access are based on the interest of reducing illegal content over the Internet. However, heavily regulated content access measures would increase the costs for intermediaries to operate Internet-related services and costs of service interruption. Pillar 9 deals with regulatory measures that stand on an ill-placed balance of these two competing objectives, as shown in figure 22.

Figure 22 **Balance in different policy objectives in Pillar 9**



With the balance between these policy objectives, the Pillar 9 consists of the following indicators:

- Blocking or filtering commercial web content;
- Internet shutdowns;
- Online advertising requirements; and
- Licensing requirements.

Blocking or filtering commercial web content

This indicator asks whether there have been any instances of blocking or filtering commercial web content either by a Government or Internet intermediaries as required by the Government:

- **'Blocking'** means denying access to a certain commercial website in its entirety;
- **'Filtering'** is limiting access only to certain online content on a given website.

Generally, a Government blocks or filters websites or web content on the grounds of 'public morality' or 'national security' in order to prevent or respond to online security threats, such as malicious network traffic. Limiting content access of commercial websites or web content on the grounds of amorphous public policy constitutes substantial burdens on businesses and online users because of the uncertainty of regulation and additional costs in managing their websites. For example:

- Viet Nam requires ISPs to remove or block information that alludes to State opposition, undermines national security and social order, conducts propaganda, and harms national traditions and customs;
- Türkiye also bans online content based on interests, including protection of national security and public order;

- Brunei Darussalam bans or requires licensed Internet service providers and online content providers to use "their best efforts" to ban online content that is against the public interest or national harmony.

The score is '1' for each blocking measure. All types and techniques of blocking, i.e., IP address and Protocol-based blocking, Deep Packet Inspection-based blocking, URL-based blocking and DNS- based blocking, are included because each type and technique leads to different outcomes, including under-blocking and over-blocking (Keller, 2018).[32] The score is '0.5' for each filtering measure. Blocking or filtering political content, criminal content (e.g., child pornography), aged-restricted content, defamation and other non-commercial content would not be scored. Blocking or filtering based on intellectual property violations, such as copyright infringement content, is not considered as a restriction because this content exploits the right holders' exclusive right and is prohibited by the law; thereby, this would not be included, either.

Useful secondary sources include the DTE database, the reports by the Global Network Initiative, the World Intermediary Liability Map, the Freedom House on the Net, the NTE reports, and complaints by companies. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Internet shutdowns

This indicator asks whether an economy imposes Internet shutdowns and the presence of Internet shutdowns occurring in the economy. Internet shutdowns refers to an internationally disruption of the Internet or online services to prevent access to information, services and products. The shutdowns can be implemented in specific parts or areas within the economy. By implementing this measure, it has a large impact on the possibilities of doing business as well as affecting the users.

For scoring of this indicator,

- The score is '1' when Internet shutdown occurs extremely often. It is a regular practice for a Government to shut down domestic access to the Internet;
- The score is '0.75' when Internet shutdown occurs often. The particular Government shut down domestic access to the Internet numerous times this year;
- The score is '0.5' when Internet shutdown occurs sometimes. The particular Government shut down domestic access to the Internet several times this year;
- The score is '0.25' when Internet shutdown rarely occurs. The particular Government shut down domestic access to the Internet on a few occasions throughout the year;
- The score is '0' when Internet shutdown is never or almost never. The particular Government does not typically interfere with domestic access to the internet.

[32] For the clarification of each blocking technique, see https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

The secondary sources should only serve to guide researchers to the primary sources. The main secondary source is Varieties of Democracy (V-Dem) variable v2smgovshut.[33]The V-Dem provides time series data in numerical answer from 0 to 4. Under V-Dem, the interpretation of the score is different from the RDTII 2.0, as follows:

- The V-Dem score of '0' refers to when Internet shutdown occurs extremely often;
- The V-Dem score of '1' refers to when Internet shutdown occurs often;
- The V-Dem score of '2' refers to when Internet shutdown occurs sometimes;
- The V-Dem score of '3' refers to when Internet shutdown rarely occurs; and
- The V-Dem score of '4' refers to when Internet shutdown is never or almost never.

To get the answer, select '6.2.4 Government Internet shut down in practice' indicator and select an interested economy (more than one economy can be selected). For parameters, select 'original scale', set show for both 'confidence rating' and 'mouseover', and choose the latest year available. Once all options have been set, the answer will appear in terms of the number and decimal on the graph, but only the number in the first line will be used (the range of the number in the second line is not listed). The data shown in the graph can be downloaded as a csv. file and only the number under the economy name column will be used.

Online advertising requirements

The indicator covers requirements on online advertising. The measures could be limitations affecting online advertising (excluding requirements that advertising should not be misleading). The regulation that is silent about the scope of the application of requirements on advertisements can be considered as also being applied to online advertising, unless it is clear that the rule applies only to offline advertisements.[34] For example:

- The Lao PDR mandates that individuals, legal entities and organizations intending to advertise goods and services must acquire approval from the information and culture sector;
- Ecuador mandates that media advertisements – for example, television and film territory by Ecuadorian natural persons or foreigners residing in Ecuador as well as by Ecuadorians residing abroad or foreign entities whose majority ownership corresponds to Ecuadorians;
- Kazakhstan prohibits advertisements that contain a comparison of the advertised goods (work and service) with the goods (work and service) of other individuals or legal entities as well as statements, images, discrediting their honour, and digital and business reputation.

The score is '1' for each requirement limiting online advertising. Otherwise, the score is '0.' Any measure related to online advertisements for the purpose of online consumer protection should also be scored '0'.

The secondary sources, such as the OECD Digital STRI should serve as guidance for the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

[33] V-Dem Codebook V.12 (as of March 2022) is available at https://v-dem.net/static/website/img/refs/codebookv12.pdf

[34] The majority of countries has advertisement regulations that do not differentiate online and offline and hence restriction is assumed to being applied to both.

Licensing requirements

This concerns a licence to licensing scheme on certain online service providers. Here, the online service providers mean the following ICPs and applications:

- Social media platforms;
- News providers (e.g., media and broadcast services);
- Virtual Private Network (VPN);
- Cloud services, etc.

This indicator excludes telecommunication facilities and service providers, which are already covered by Pillar 5, as well as e-commerce platforms which are covered by Pillar 12. It asks whether (a) the ICPs are subjected to licensing requirement to operate their business, and (b) whether the licensing requirement is considered as a "strict" requirement, in that they have the potential to block businesses from operating their services.

- The strict licensing schemes. For example, Pakistan requires a licence for broadcasting media and distribution services. However, such a licence is prohibited to a person who is not a citizen or a resident in Pakistan, a foreign company, a company with the major shares owned or controlled by foreign natural or juristic persons, and any person funded or sponsored by a foreign Government or organization. Viet Nam requires an online social network to establish a company in Viet Nam in order to register for a licence from the Ministry of Information and Communication of Vietnam.

The non-strict licensing scheme. For example, Nepal requires online news companies to register at the Department of Information and Broadcasting. Online radio, television and on-demand streaming services such as YouTube and Netflix, and online news sites, are required to obtain a licence from Türkiye's government-controlled State television and radio regulator, the Radio and Television Supreme Council (RTÜK). The score is '1' for a strict licensing scheme. The score is also '1' if the economy implements more than one licensing requirement. The score is '0.5' if the economy implements a licensing scheme. Otherwise, the score is '0.'

The secondary sources include the DTE database, the reports by the Global Network Initiative, the Freedom House on the Net, the World Map of Encryption Laws and Policies, and the NTE reports. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

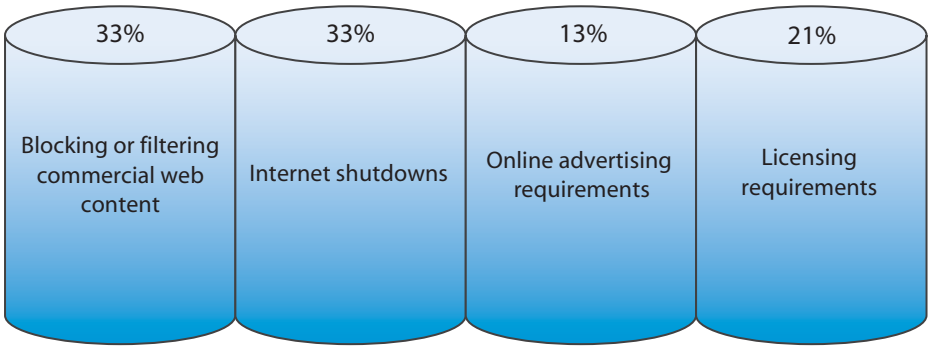
The weights for each indicator

As shown in figure 23, weights of each indicator related to the Internet intermediaries are 33%, 33%, 13% and 21%, respectively. The first and the second indicators equally receive the highest weight of 33%. Blocking or filtering, and Internet shutdowns directly interrupt the intermediaries from performing their services as well as having an impact on the end-users. The third and the fourth indicators on the requirements for an online advertising and licensing scheme potentially discourage the Internet intermediaries without impeding their services, thereby receive a lesser weight of 13% and 21%, respectively. Although online advertising requirements limit the intermediaries' performance and could affect the engagement with customers, the intermediaries

are still able to operate their services. Under the licensing requirements, the intermediaries may not be permitted to operate any activities unless they obtain a licence. The licence is also costly as it involves time and procedures.

Figure 23

Pillar 9 indicators and the weights



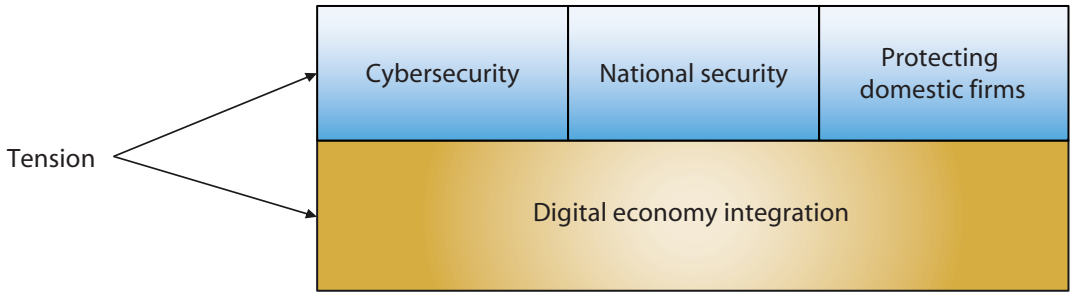
Pillar 10. Non-technical NTMs

Pillar 10 captures non-technical NTMs, including measures other than tariffs or taxes that limit the importation and exportation of ICT goods and online services from the economies within the considered United Nations region. These measures, such as bans, quotas and licensing procedures, could reduce the flow of ICT goods and online services.

Some of such measures are put in place based on the interests of protecting public order, cybersecurity and national security. For example, import bans on certain applications are designed to cut off cybersecurity as well as national security threats that they pose to the domestic networks. Certain export bans prohibit exports of certain ICT products and technologies that the economies consider to be vital to the interests of their nations. Other measures under this Pillar are for the purpose of guarding the domestic market against potential foreign market power. For example, local content requirements imposed on imports push foreign suppliers to acquire components that are to be built into their products from domestic suppliers. However, these policy objectives stand in tension, as shown in figure 24.

Figure 24

Tension among different policy objectives in Pillar 10



Pillar 10 aims to reveal specific areas of non-technical NTMs that this type of tension creates by covering the following indicators:

- Import bans;
- Other import restrictions;
- Local content requirements; and
- Export restrictions.

Import bans on ICT goods and online services

This indicator looks at import bans on ICT goods and online services. The score is '0.5' if there is only one ban covering one specific product. If there is more than one measure or the measure covers more than one product, the score is '1'. The score is '0' if there is no such measure.

Secondary sources include WTO I-TIP, the Global Trade Alert database, the U.S. Country Commercial Guides, the NTE report and complaints by companies and associations. The secondary sources should only serve to guide researchers to the primary sources.

Other import restrictions on ICT goods and online services

This indicator covers import restrictions, excluding other than import bans and local content requirements on imports:

- Measures such as import quotas are trade-blocking, limiting the volume of ICT goods or online services that can be imported;
- Measures such as import licensing schemes and procedures do not necessarily block imports *per se*, but discourage the trade in ICT goods. They create additional costs and delay the import process. For example, Pakistan allows only companies that have an agreement with the Government or licensed authorities on import transmission apparatus for radio broadcasting or television, television cameras, digital cameras and video camera recorders. In Botswana, the Communications Regulatory Authority (BOCRA) is mandated to approve communications equipment that may be connected, used or operated to provide broadcasting or telecommunications services in Botswana. In Argentina, non-automatic import licences for ICT goods such as machines and apparatuses for the manufacture of semiconductors entail a more complex import process, in which additional documentation and the intervention of technical agencies can take place. In Haiti, individuals of foreign nationality involved in importing are obliged to obtain a licence, which must be renewed at the start of every fiscal year.

The score is '0.5' for each restriction that adds regulatory compliance costs to trade in ICT goods and online services, such as licences, permits, authorization and registration for ICT goods, and labelling requirements and import controls, both for ICT goods and online services.[35] The score is '1' for trade-blocking measures such as quotas, or if there are two or more measures that incur additional business costs. Otherwise, the score is '0' if none of the above measures are implemented and there appears to be institutional transparency in the import procedures.

Researchers should look at official laws, regulations, notifications, and other measures. The secondary sources are WTO I-TIP, the Global Trade Alert databases, the U.S. Country Commercial Guides, the NTE report, as well as reports by by international organizations. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Local content requirements for the commercial market

This indicator covers **'local content requirements'** (LCRs), i.e., requirements to use domestically manufactured goods or domestically supplied services in the production of ICT-related goods and online services. The LCRs under this Pillar do not include the measures implemented for public procurement tenders, which are covered by Pillar 2. For example:

- The Russian Federation sets an annual minimum volume of purchases by SOEs of innovative and high-tech products;

[35] For clarification of each type of import-related procedure, see UNCTAD International Classification of Non- Tariff Measures, available at https://unctad.org/system/files/official-document/ditctab2019d5_en.pdf.

- Argentina has local content requirements for certain products (such as technical manuals, packaging and labels) in the production of mobile and cellular radio communication equipment operating in Tierra del Fuego province;
- Indonesia requires telecom operators to expend a minimum of 50% of their total capital expenditures for network development on locally sourced components or services;
- Indonesia requires Internet protocol set-top-boxes with a minimum local content requirement of 20% and a gradual increase to 50% within five years.

The score is '0.5' when LCRs apply at the product level, i.e., HS-6 and HS-8 levels (e.g., mobile phones and smartphones).[36] The score is '1' if there are two or more LCRs at the product level, or if the LCRs apply at the sectoral or horizontal level, i.e., HS-4 (e.g., telephony equipment) and HS-2 levels. The score is '0' if there are no LCRs in this area.

Researchers should look at official laws, regulations, notifications and other measures of relevant ministries. Secondary sources such as WTO I-TIP, the Global Trade Alert database, the U.S. Country Commercial Guides, the NTE report, as well as complaints from companies and trade associations should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Export restrictions on ICT goods and online services

This indicator covers export restrictions on ICT goods and services. These restrictions include export bans, export licences and other restrictions limiting the number of goods or services to be exported. For example:

- India and the Republic of Korea export licence on strategic items, including the dual-use items of computers, telecom and information security;
- Colombia prohibits the export of smartphones, with some exceptions such as mobile phones that are personal possessions of travellers, among others;
- Hong Kong, China imposes export permits on radio transmitting apparatus;
- Thailand requires an export license for radio communication equipment and ancillary devices.

The score is '1' if at least one of such measures is implemented. Otherwise, the score is '0'.

Researchers should look at official laws, regulations, notifications and other measures of relevant ministries. Secondary sources, such as WTO I-TIP, the Global Trade Alert database, the OECD Inventory on Export Restrictions on Industrial Raw Materials, the U.S. Country Commercial Guides, the NTE report, as well as complaints from companies and trade associations should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

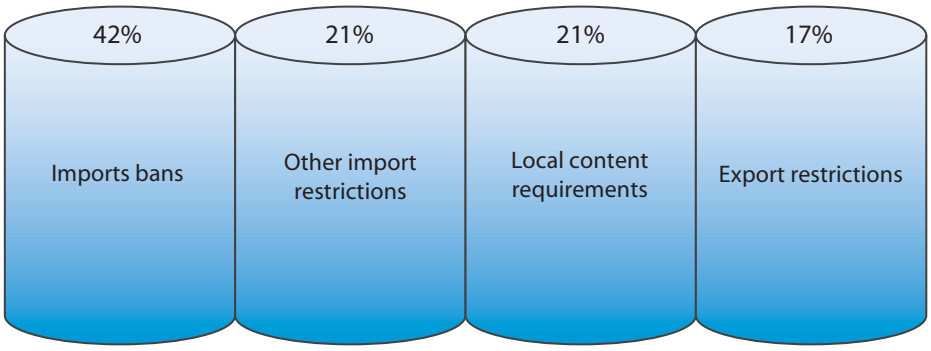
[36] Harmonised System (HS) is an international nomenclature provided by the World Customs Organization (WCO) for the classification of products. The HS Code adopted a six-digit code system to classify goods (WCO, 2016).

The weights for each indicator

As shown in figure 25, the weights of each of the indicators are 42%, 21%, 21% and 17%. The first indicator on import bans gets the highest weight of 42% as it completely prohibits imports. Indicators on other import restrictions and local content requirements equally receive a lesser weight of 21% because these measures limit the flows of ICT goods and online services as well as discriminate against foreign businesses. Other import restrictions hinder trade facilitation by imposing additional import procedures. Local content requirements require foreign companies to use domestic resources according to the prescribed threshold, increasing costs and barriers for the companies to find suitable local materials or services for their supply chains. Each of the measures directly undermines foreign competition in the domestic market, while the last indicator, on export restrictions, has a limited impact on foreign competition in the economy concerned and is thereby given the least weight of 17%.

Figure 25

Pillar 10 indicators and the weights

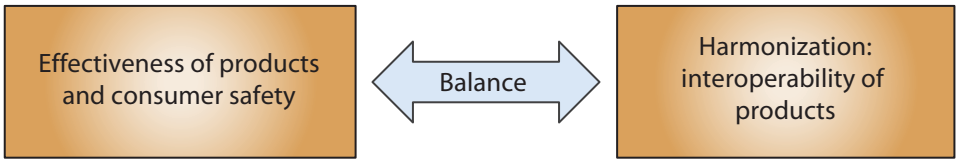


Pillar 11. Standards and procedures

Pillar 11 covers technical standards and related procedures that can function as a trade restriction on ICT goods and online services in a digital economy, specifically in the telecommunication sector. Technical standards ensure the effectiveness of products and consumer safety by setting out minimum requirements necessary to ensure the quality of products or services. However, disparate technical standards and related procedures across the region undermine this interoperability and thereby discourage digital trade due to higher trade costs and delayed processes. Adopting technical standards that are internationally recognized as best practices increases the interoperability of products and services across the region (figure 26).

Figure 26

Balance in different policy objectives in Pillar 11



Pillar 11 measures the interoperability of regulation in the following indicators:

- Lack of transparent technical standards;
- Self-certification limitations for product safety (radio transmissions, EMC/EMI);
- Product screening and testing requirements; and
- Deviation from international encryption standards.

Lack of transparent technical standards

In developing an open and transparent technical standards regime, all relevant stakeholders should be able to engage and provide comments. This indicator asks whether (a) foreign participation is not allowed in standard-setting of the technical standards applied to ICT goods and online services in sectors relevant to digital trade, including the telecommunication sector, and (b) whether the standard-setting is not transparent.

- The limit on foreign participation. For example, in Cuba, foreign companies are not allowed to participate in institutional bodies that establish and regulate trade norms. Egypt requires that the board of directors of the National Telecommunication Regulatory Authority is authorized to set standards for telecom equipment without foreign participation.
- The lack of institutional transparency of technical standards setting can be found in various forms. For example, Australia requires, that a participant in technical committees that develop standards for electrical products must have its headquarters based in Australia and have an Australian membership base. In the case of Burundi, the fact that not all national standards are based on a common worldwide basis could still create inefficiencies in the market, which result in higher trade costs.

This indicator has binary scores, '0' or '1'. The score is '1' if foreigners are not allowed to participate in the standard-setting bodies or if standard-setting is not transparent. Researchers should look at official laws, regulations and other measures. Secondary sources such as complaints from companies and trade associations as well as the NTE report should only serve to guide researchers to the primary sources.

Self-certification limitations for product safety (radio transmissions, EMC/EMI)

This indicator asks whether self-certification of product safety by suppliers is not allowed. In general, exports of electrical products must comply with domestic standards of radio transmissions, electromagnetic interference (EMI) or electromagnetic compatibility (EMC).[37]

Economies allow the self-certification of the products to vary degrees. Generally, economies implement the following measures for self-certification:

- Self-certification through **'Supplier Declaration of Conformity'** (SDoC) ensures compliance with the prescribed domestic standards;
- Third-party certification from **'Conformity Assessment Bodies'** (CABs) does away with the need for local testing of the products to be exported. Generally, economies that are members of a Mutual Recognition Agreement (MRA), such as the ASEAN MRA for Electrical and Electronic Equipment (ASEAN EE MRA) and APEC MRA for Conformity Assessment of Telecommunications Equipment (APEC TEL MRA), maintain reciprocity in recognizing CABs in their territories (ASEAN, 2012; FCC, 2016).

The score is '1' if an economy recognizes neither self-certification nor third party-certification and requires foreign suppliers to undergo testing in a local laboratory. The score is '0.5' if a SDoC is not permitted, but the third-party certification from CABs in other economies is accepted. The score is '0' if a SDoC is permitted for foreign businesses.

Researchers should look at official laws, regulations and other measures. Secondary sources such as the DTE database, the U.S. Country Commercial Guides, the reports by business associations and from the Telecommunication Industry Association (TIA) (which represents manufacturers and suppliers of global communication networks) and the International Telecommunication Union (ITU) should serve only to guide researchers to primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Product screening and testing requirements

The indicator asks whether an economy imposes an additional screening or testing requirement on ICT imports. The declared justifications for these requirements are often about national security.[38] For example:

[37] The EMC testing measures whether electrical devices can function in the environment without interfering with surrounding equipment by emitting radiation. While the EMI testing gauges whether electrical products can function in the presence of a certain amount of electromagnetic interference. Different requirements and interpretations of the definition of EMC and EMI in the United States and the European Union could cause confusion when it comes to testing (Hayes, 2021).

[38] Thus, these requirements are distinguishable from testing or screening requirements based on the interest of public safety and efficiency of products such as EMC or EMI testing requirements.

- New Zealand requires companies that use 5G network equipment to receive approval under security assessment by the Government Communications Security Bureau to prevent the harm that may affect national security;
- India requires onerous in-economy security testing on all telecom network equipment and products. Previously, such products used to be tested and certified in laboratories globally or at in-house laboratories of the manufacturers;
- The Republic of Korea imposes security verification requirements on imports of network equipment and cyber-security software. Although the certification of the products from a Common Criteria Recognition Arrangement (CCRA) accredited laboratory outside the Republic of Korea can satisfy the requirement, the Common Criteria (CC) certification may not be sufficient for two reasons. First, the Government may substitute the CC certification with other certification mechanisms that were internally developed (e.g., GS Certification). Second, it may reject a CC certification when it deems that the certification does not cover particular functions of the product that the Government entity needs. Furthermore, certain network equipment must undergo an additional security verification process;
- The Russian Federation requires equipment and devices containing encryption to be registered with the Federal Security Service (FSS) as well as the manufacturer or the seller to obtain FSS notification upon importation or exportation of such equipment. Notification of the FSS is a prerequisite for the import into the territory of the Eurasian Economic Union (EAEU) or export from the territory of the EAEU of equipment containing encryption elements;
- Thailand requires telecommunication equipment to be tested to ensure that the products conform to the technical standard prescribed by the national agency. The agency recognizes both local and foreign testing laboratory results that conform to the required conditions;
- The Gambian standards generally require local testing for electrical products for certification. Audio and video products such as televisions, LCD panels and similar apparatus marketed in The Gambia are required to undergo local testing. Audio and video products are certified only after conformity assessments have been carried out by The Gambia Standards Bureau (TGSB).

If a requirement for domestic screening or testing exists, the score is ‘1’. If third-party testing results are accepted by local authorities, the score is ‘0.5’. The score is ‘0’ if there is no requirement for screening or testing.

Researchers should look at official laws, regulations, notifications, and other measures. Useful secondary sources include the DTE database, the U.S. Country Commercial Guides, and reports by business associations and from the Telecommunication Industry Association (TIA) and the International Telecommunication Union (ITU). The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Deviation from international encryption standards

The indicator covers requirements on encryption standards. Encryption is the process of encoding a message or information with an algorithm by converting original text (known as plaintext) to an alternative form (known as ciphertext).[39] Decryption, in turn, is the process of accessing the plain text of the encrypted message requiring a password or a **'private key'**. The objective of encryption is to secure data and prevent data breaches. The encryption strength is based on the key's size, length and design.

Specifically, the indicator asks the following questions: (a) whether an economy adopts encryption standards that deviate from internationally recognized standards (box 6); and (b) whether an economy has requirements to disclose trade secrets or sensitive proprietary information in the process of certifying products that contain.

Encryption:

- The encryption standards that deviate from international standards appear in various forms, such as the requirement to adopt domestic encryption standards and the condition to use lower standard bits block ciphers. For example, China requires foreign suppliers of network equipment and mobile devices comprising 4G TD-LTE networks to use domestically developed encryption algorithms, such as ZUC, although a globally accepted standard already exists (3GPP).[40] India requires companies to use a 40-bit or lower standard encryption to secure digitally transmitted information unless they must procure a licence. Senegal requires that private use of cryptography software will be within the key length inferior bits, unless they will be subjected to a declaration regime.
- The disclosure of trade secrets when certifying encryption products. For example, the Republic of Korea requires that the suppliers of software systems and hardware equipment (e.g., VPN and firewall systems) to be used in the Government must submit the source code to receive the verification test.

The score is '1' if at least one of such measures is implemented. Otherwise, the score is '0'.

Researchers should look for official laws, regulations, notifications, and other measures. Secondary sources include the World Map of Encryption Laws and Policies, the reports of the Freedom House on the Net and the DTE database. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

[39] Encryption is a principal application of cryptography. Cryptography refers to the technological means to secure information and communications systems (OECD, 2022).

[40] 3GPP (3rd Generation Partnership Protection) develops mobile broadband standards, such as GSM, LTE and 5G specifications (3GPP, 2008).

Box 6

International encryption standards for import encryption methods

There are myriad types of encryption algorithms or the methods of transforming plain text to ciphertext as well as the international encryption standards. Several institutions have established international encryption standards, i.e., the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), ITU, Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST). The international standards set out by these institutions include standards for the design and validation of hardware and software cryptographic modules (ISO/IEC 19790:2012 and ISO/IEC 24759:2017), standards ensuring data confidentiality (ISO/IEC 18033-3), standards ensuring information security management (ISO/IEC 27000), and standards specifying symmetric encryption to use algorithms of 64-bits block cipher and 128-bits block cipher (ISO/IEC 18033-3: 2005). Significantly, these international encryption standards serve as a baseline for the encryption algorithms.

Encryption algorithms can be classified into **'symmetric key based'** and **'asymmetric key based'**. First, symmetric encryption algorithms refer to when there is one private key for both encryption and decryption. The commonly used algorithms under this type are, for example, the Advanced Encryption Standard (AES) that is used to protect data, and sensitive data with cryptographic keys of 128, 192 or 256 bits to encrypt and decrypt data in blocks of 128 bits; and the Triple Data Encryption Standard (TDES) that is used in financial services to encrypted transactions by triplicate encrypting with cryptographic keys of 56 bits (168 bits) to encrypt and decrypt data in blocks of 64 bits. Both AES and TDES are specified under the ISO/IEC 18033-3:2005 regarding their block and key lengths.

Second, asymmetric encryption algorithms refer to when there are two separate keys, including private and public keys, each for encryption and decryption. The commonly used algorithms under this type, for example, Elliptic Curve Cryptography (ECC), are generally used for digital signatures and web applications. The ECC is also specified under ISO/IEC 29167-16:2015 for describing a crypto suite based on this encryption algorithm.

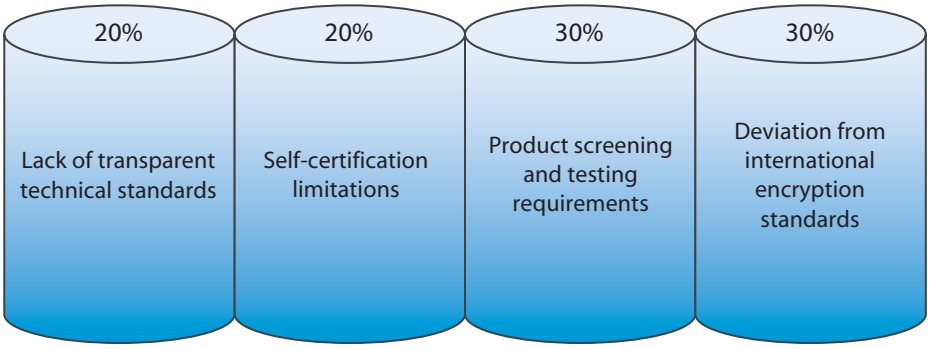
The weights for each indicator

As shown in figure 27, the weights are 20%, 20%, 30% and 30%, respectively. The third and fourth indicators are assigned similar weights of 30% because each indicator has the potential to discourage foreign businesses from operating in certain economies. As new digital technologies are increasingly emerging, standard-setting on ICT goods and online services is crucial for creating an integration system and timely response to technological developments. Divergent domestic approaches to standards and compliance procedures of self-certification and testing requirements could result in inconsistent quality and safety of the end-products or services in the market. The first and the second indicators receive a lesser weight compared with 20%. Although self-certification requirement and screening requirements provide additional layers and thus slow down the process, the product screening and testing requirements could further result in a ban on the imported ICT goods or prohibition of certain online services. The screening and testing mechanisms are generally based on the reason of national security, and thereby could create

uncertainty. The requirement on encryption standards and trade secrets not only leads to a lack of interoperability as it does in the technical standards regime. The encryption in relation to data confidentiality of the data storage and data transmission against unauthorized access as well as the mandatory disclosure of trade secrets creates impacts on business competition.

Figure 27

Pillar 11 indicators and the weights

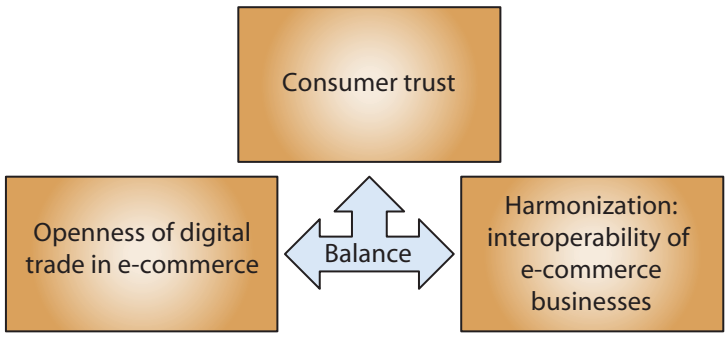


Pillar 12. Online sales and transactions

Pillar 12 captures requirements for online sales and transactions. The steady increase in online sales and transactions over the years, both in developed and developing economies, reflects how critical these flows have become for digital trade. Measures surrounding electronic commerce in the areas of, foreign investment, online sales, delivery, licensing requirement, online payment, *de minimis* rule, domain names and local presence requirements may limit digital trade as these are essentials to set up and operate an e-commerce business in the regulating economy. Furthermore, the lack of legal recognition for electronic communication, signatures and transactions cuts back digital trust and undermines the interoperability of e-commerce businesses in the region. Finally, the presence of consumer protection laws in the e-commerce sector increases consumer trust and, thereby, participation in digital trade by foreign vendors in the regulating economy. Sound policies for e-commerce find a balance among these policy objectives, as shown in figure 28.

Figure 28

Balance in different policy objectives in Pillar 12



Based on this understanding, Pillar 12 reflects the following issues:

- Foreign equity limits in e-commerce sector;
- Online purchases and delivery limitations;
- Licensing requirements in e-commerce sector;
- Online payment limitations;
- Low De Minimis;
- Domain name requirements;
- Local presence requirements;
- Lack of a legal framework for online consumer protection;
- Not in the UN Convention on Electronic Communications;
- Not in the UNCITRAL Model Law on Electronic Commerce; and
- Not in the UNCITRAL Model Law on Electronic Signatures.

Foreign equity limits in the e-commerce sector

This indicator concerns maximum foreign equity shares in the specific sector of e-commerce. Foreign equity shares are shares that foreign natural or legal persons hold in a firm incorporated in the investee economy. Limitation on foreign equity shares is a direct obstacle for foreign investors that could induce a higher level of development in the e-commerce sector. For example, the Philippines bans foreign ownership of retail trade enterprises with paid-up capital of less than US$ 2.5 million.

In particular, the foreign equity shares under this Pillar do not include the foreign equity shares in other sectors relevant to digital trade or the telecommunication sector, which are captured in Pillars 3 and 5, respectively. According to a specific focus on e-commerce, the scoring metric on State-owned enterprises is not included.

The score is '1' if only a minority stake (less than 50%) is allowed. The score is '0.5' where a controlling stake (more than 50%) is allowed, but maximum caps on foreign equity exist. The score is '0' if there is no limitation on foreign equity share in e-commerce sector.

Online purchases and delivery limitations

The indicator covers requirements on online purchases and the requirements on the delivery of products bought online. The measures could be:

- Specific limits on the number of goods imported by customers through e-commerce platforms. For example, Brazilian Customs have established express services maximum per-shipment value limits of US$ 3,000 for imports, while in Argentina, consumers can purchase goods valued at up to US$ 50 per month tax-free, with an annual tax-free limit of US$ 600. If the monthly purchase total exceeds US$ 50, the consumer must pay a 50% tax on the value above the US$ 50 threshold;
- Specific limits on the number of goods to purchase through e-commerce platforms;
- Limitations on the delivery of products bought online applied to the delivery company. For example, Indonesia requires a foreign postal operator to cooperate with a domestic postal operator through joint ventures and they are prohibited from operating intercity delivery services;
- Limitations on the delivery of products bought online applied to the users.

The score is '1' for each requirement limiting the number of purchases via e-commerce or delivery. Otherwise, the score is '0.'

Researchers should look at official laws, regulations, and other measures. Secondary sources, such as the OECD Digital STRI and the U.S. Country Commercial Guides, should serve as guidance for the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Licensing requirements in the e-commerce sector

The indicator covers any licensing scheme for e-commerce providers, including both business-to-business (B2B) and business-to-consumer (B2C) platforms.

For example:

- India requires foreign companies relating to B2B, B2C e-commerce, data interchange, digital supply transactions, web-based marketing, database services, online services and related data communication services, even when they are not incorporated in India, should register in India when they are engaged in business in the economy;
- Thailand requires that websites involving the transaction of goods and services, for example, electronic business operating in the Internet system, service providers, web hosting, e-Marketplace or platform, to register with the Department of Business Development;
- Colombia requires web pages and Internet sites of Colombian origin whose activity is of a commercial, financial or service nature to be registered in the commercial registry, and to provide the National Tax and Customs Directorate with information on their economic transactions; and
- The Lao PDR requires existing and new e-commerce businesses that trade through their platforms or electronic marketplaces to register at the Ministry of Industry to receive an acknowledgement certificate.

The score is '1' for each licensing for e-commerce providers. Otherwise, the score is '0.'

Researchers should look at official laws, regulations, and other measures. Secondary sources, such as the OECD Digital STRI and the U.S. Country Commercial Guides should serve as guidance for the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Online payment limitations

The indicator covers requirements for online payments and other requirements affecting the use of electronic payment and credit services. Such requirements are diverse:

- Requirements to use a local bank account;
- Requirements on the currency used for international payments;
- National standards for payment security that deviate from international standards;
- Ceilings on the maximum amount that can be paid by electronic payment methods; and
- Requirements mandating the use of specific intermediaries for online payments.

For each measure, the score is '1'. Otherwise, the score is '0'. Requirements for 'cryptocurrencies'[41] are not listed since the implication for using this type of payment is relatively new and still lacks concrete evidence.

Researchers should look at official laws, regulations and other measures. Secondary sources, such as the OECD Digital STRI, should serve as guidance for the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

[41] Cryptocurrencies, a subset of virtual currencies, adopt blockchain or distributed ledger transactions (DLT) to process virtual transactions. The entire concept of digital currency is available at (ESCAP, 2017); see also Houben and Snyers, 2018.

Low de minimis

The indicator asks whether an economy adopts a threshold for *de minimis* rule. The *de minimis* rule sets a valuation ceiling for goods below which no duty or tax is charged at the border to ensure the flow of digital trade. According to the International Chamber of Commerce (ICC) recommendation of establishing a global baseline of *de minimis* value, the index calculates the valuation ceiling based on a US$ 200 threshold (ICC, 2016).

If no *de minimis* rule exists, a score '1' is given. If an economy adopts the *de minimis* rule below US$ 200, a score '0.5' is given.[42] However, if the *de minimis* rule is equal to or above US$ 200, a score of '0' is given. For consistency across datasets, the exchange rates should be based on the International Monetary Fund (IMF).

Researchers should look for relevant official laws, regulations, notifications and other measures. A useful secondary source is a Global Express Association database. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Domain name requirements

The indicator covers requirements on commercial domain names.[43] These requirements may have costs of compliance. They include requirements for companies to have a local domain name to engage in electronic retail in a certain market, requirements to establish a local presence as a condition for using a local domain name, and requirements to appoint a local representative.

For example:

- Malaysia requires that the registrant of a ".my" domain must have a valid proof of residence in Malaysia;
- Kazakhstan requires that registrant of ".kz" or ".kaz" domains must be hosted on a server in a data centre located within the economy;
- Thailand requires that a foreign juristic person registrant of ".co.th" must appoint a local agent to hold right rights in domain name on behalf;
- In Brazil, foreign companies aiming at registering a domain must have a representative in the country to register before the country's official registry administrator for domain names.
- Singapore requires that a foreign registrant of ".sg" domains must appoint a local agent with a valid postal address within the economy.

All hierarchies of domain names are included. However, the domain names for government agencies, military, educational institutions or other organizations, namely '.gov', '.mil', '.edu' or '.org', are not listed because they do not focus on commercial activities.

[42] SDR is a calculated deflator based on inflation measures of the economies represented in a basket of currencies and takes stock of international inflation and exchange rates.

[43] A domain name system (DNS) links the online users to each IP address, which is a string of numerical digits and periods, by providing a familiar string of letters known as the 'domain name'. A domain name includes different types and hierarchies: Top-Level Domains (TLDs), Second-level domains and Third-level domains.

A score of '1' is assigned if a physical presence is required to use a local domain name or if companies are required to obtain a local domain name in order to engage in electronic commerce business. A score of '0.5' is given if companies are mandated to appoint a local administrative. If there are no requirements on domain name, the score is '0'.

Researchers should look at official laws, regulations and other measures. Secondary sources such as the OECD Digital STRI database should serve as guidance for the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Local presence requirements

This indicator asks whether an economy imposes local presence requirements on online service providers. The **'local presence requirement'** requires companies to have a representative office, local agent, legal representative or a post-box within the economy to provide their services. For example, Indonesia requires Private Electronic System Operators (ESOs) to register their businesses at the relevant ministry. The ESOs should appoint liaison officers who have domicile in Indonesia to facilitate any access request by the government authorities. For example, Türkiye requires foreign-based social network providers whose platforms are accessed from within Türkiye more than one million times a day to appoint a real or legal person representative in Türkiye.

For scoring, if there is local presence requirement, the score is '1'. Otherwise, the score is '0'. Researchers should look at official laws, regulations, and other measures. The secondary sources include the DSTRI database, and the NTE reports. The secondary sources should only serve to guide researchers to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Lack of legal framework for online consumer protection

This indicator asks whether an economy has adopted an online consumer protection legal framework. The domestic laws of consumer protection need not be specific to e-commerce. A law that applies to transactions across sectors for the purpose of protecting consumers can extend to e-commerce transactions under its umbrella. The consumer protection law applicable to online purchases can be found within the same protection provided to the offline transaction or in a separate regulation.

The score is '1' if an economy lacks online consumer protection legal framework or if the economy lacks consumer protection laws that are applicable to online purchases. The score is '0' for the presence of online consumer protection laws.

Researchers should look for official laws and regulations. UNCTAD Cyber Tracker database is a useful secondary source that can guide researchers' attention to the primary sources. In cases where direct access to the primary sources is not available, secondary sources may be referenced. However, researchers are advised to minimize reliance on the secondary sources and cross-check with other secondary sources before being taken into consideration.

Not in the UN Convention on Electronic Communications

The indicator asks whether an economy has signed and ratified the United Nations Convention on the Use of Electronic Communications in International Contracts (2005) (the Electronic Communications Convention). The Electronic Communications Convention is a binding treaty which requires member economies to recognize the legal validity and enforceability of electronically concluded contracts and other communications exchanged electronically (UNCITRAL, 2018c) (box 7).

If the economy has not signed and ratified the mentioned international framework, the score is '1'. If the economy has signed but not ratified the framework, then the score is also '1'. If an economy has signed and ratified the Convention, the score is '0'.

To see the status of the Convention, check the UN Convention on the Use of Electronic Communications in International Contracts (status) or the official government website.

Not in the UNCITRAL Model Law on Electronic Commerce

The indicator asks whether an economy has adopted the UNCITRAL Model Law on Electronic Commerce (1996) (MLEC). The MLEC is a model law on which an economy may base its legislation fully or in part. The MLEC establishes rules for the formation and validity of contracts concluded by electronic means, attribution of data messages, acknowledgement of receipt, and determining the time and place of dispatch and receipt of data messages (UNCITRAL, 2018a) (box 7).

If the economy has not adopted any parts of the mentioned international legal framework, the score is '1'. If the economy has adopted fully or in part of the Model Law, then the score assigned is '0'. The adoption status of the UNCITRAL Model Law is based on the list of enactments communicated to the UNCITRAL Secretariat.

To see the status of the model law, check the UNCITRAL Model Law on Electronic Commerce (status) or the official government website.

Not in the UNCITRAL Model Law on Electronic Signatures

The indicator asks whether an economy has adopted the UNCITRAL Model Law on Electronic Signature (2001) (MLES). Similar to the MLEC, the MLES is a model law on which an economy may base its legislation fully or in part. The MLES establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures as well as basic rules of conduct that may serve as guidelines for assessing duties and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process (UNCITRAL, 2018b) (box 6).

If the economy has not adopted any parts of the mentioned international legal framework, the score is '1'. If the economy has adopted fully or in part of the Model Law, then the score assigned is '0'. The adoption status of the UNCITRAL Model Law is based on the list of enactments communicated to the UNCITRAL Secretariat.

To see the status of the Model Law, check the UNCITRAL Model Law on Electronic Signatures (status) or the official government website.

Box 7

Relationship among the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures and the United Nations Convention on the Use of Electronic Communications

The MLEC is the first model legislative text that adopts the principles of non-discrimination, technological neutrality and functional equivalence. The principle of non-discrimination provides that a document must not be denied legal validity or enforceability solely on the grounds that it is in electronic form. The principle of technological neutrality mandates the adoption of neutral legislative provisions regarding the technology used. The functional equivalence principle recognizes that document and paper- based communications are given the same effect as their electronic counterparts. The MLES applies the three principles established by the MLEC in recognizing the legal validity of electronic signatures.

The Electronic Communications Convention builds particularly on the MLEC and MLES and incorporates the principles of non-discrimination, technological neutrality, and functional equivalence. Certain provisions of the MLEC were amended by the Electronic Communications Convention in light of recent electronic commerce practices. As of 2023, 18 States were parties to the Convention.

The weights for each indicator

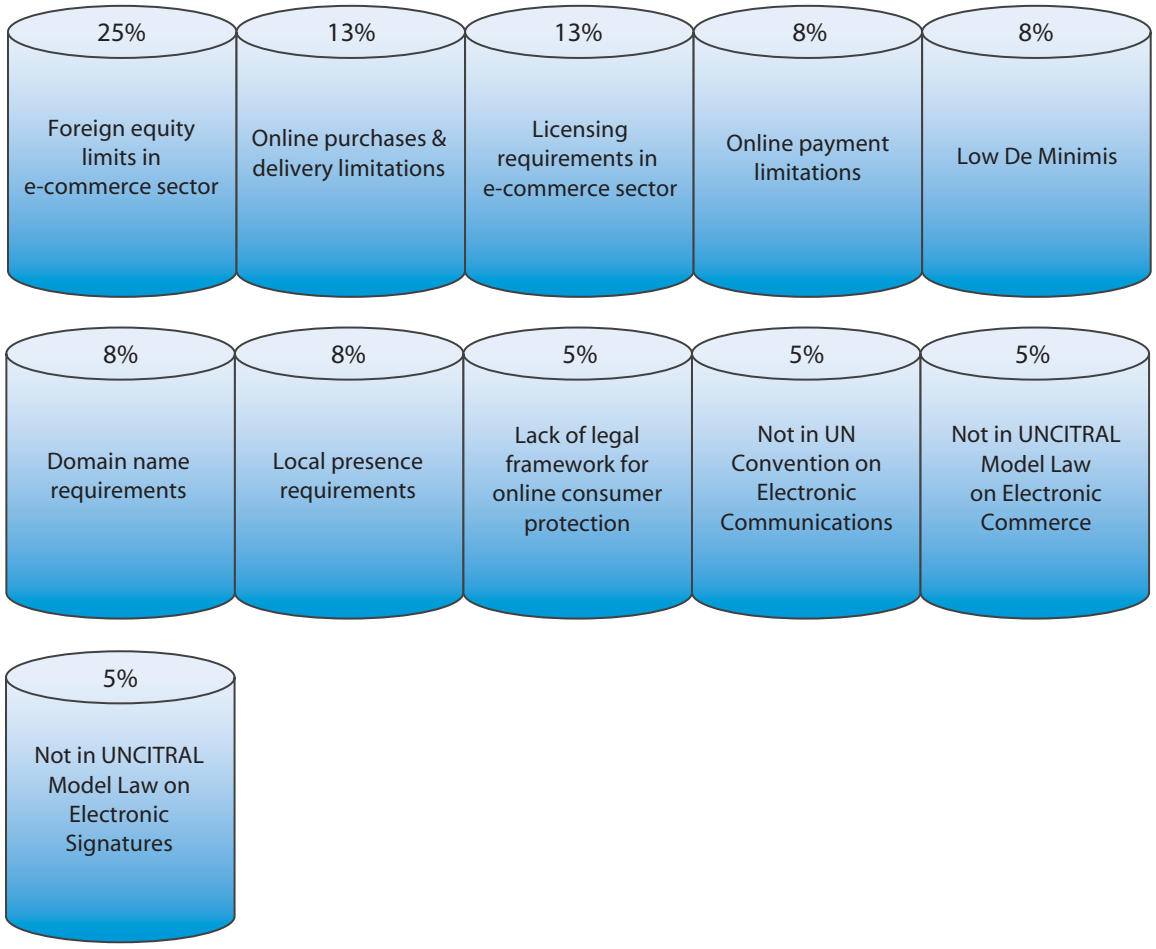
As shown in figure 29, the weights for each indicator are 25%, 13%, 13%, 8%, 8%, 8%, 8%, 5%, 5%, 5% and 5%. Maximum foreign equity shares for investment in the e-commerce sector, the first indicator, is given the greatest weight of 25% because limitations on foreign ownership discriminate and block foreign investment in e-commerce sector.

The second and the third indicators – requirements on online purchases and delivery, and licensing schemes for e-commerce providers – are equally assigned an equal weight of 13%. The requirements on sales *per se* or requirements on delivery set up direct barriers for vendors to engage in digital trade or reach consumers. Although e-commerce licensing improves reliability and confirms the existence of the business, the requirement is costly, and a rejection of licensing could preclude the e-commerce business from operating in certain economies.

The fourth indicator to the seventh indicator, which are online payment limitations, low *de minimis*, domain name requirements and local presence requirements are given a lesser weight of 8%. Each of them does not necessarily block sales or promotion of goods but discourages e-commerce activities. The requirements for online payments could make cross-border payments in electronic commerce cumbersome. The low *de minimis* rule does not block flows of goods but tends to increase the prices of imports. The domain name requirements, covering the commercial presence or a local presence requirement to purchase the local domain names, increase compliance costs. The use of national domain also correlates with engagement of the locals and the businesses. Moreover, the local presence requirements for online service providers have an impact on businesses, especially SMEs.

Last, the eighth indicator to the last indicator is given the same weight of 5% since the lack of a consumer protection law that applies to electronic commerce undermines trust in the eyes of consumers. The lack of legal recognition of electronic communications, transactions and signatures creates uncertainty in the eyes of vendors. The international frameworks facilitate harmonize e-commerce regulations and practices; however, the absence of a legal framework or the participation are not as impactful in terms of increasing the business compliance costs as the other indicators.

Figure 29 **Pillar 12 indicators and the weights**



Chapter 4

Concluding remarks

The RDTII 2.0 guideline is aimed at professionals grappling with defining the scope of the digital trade regulatory environment and how to get better evidence to develop a shared and informed vision of the risks in their particular regulatory context. The RDTII 2.0 with its 12 pillars provides a roadmap developing a sound digital trade ecosystem and a direction towards reducing regulatory-induced barriers, and the compliance costs facing businesses in the digital age, including through increasing interoperability and harmonizing regulations. Individual economies may use it as the basis for national, bilateral and regional consultations to gradually develop a digital trade regulatory environment that best meets their needs and priorities.

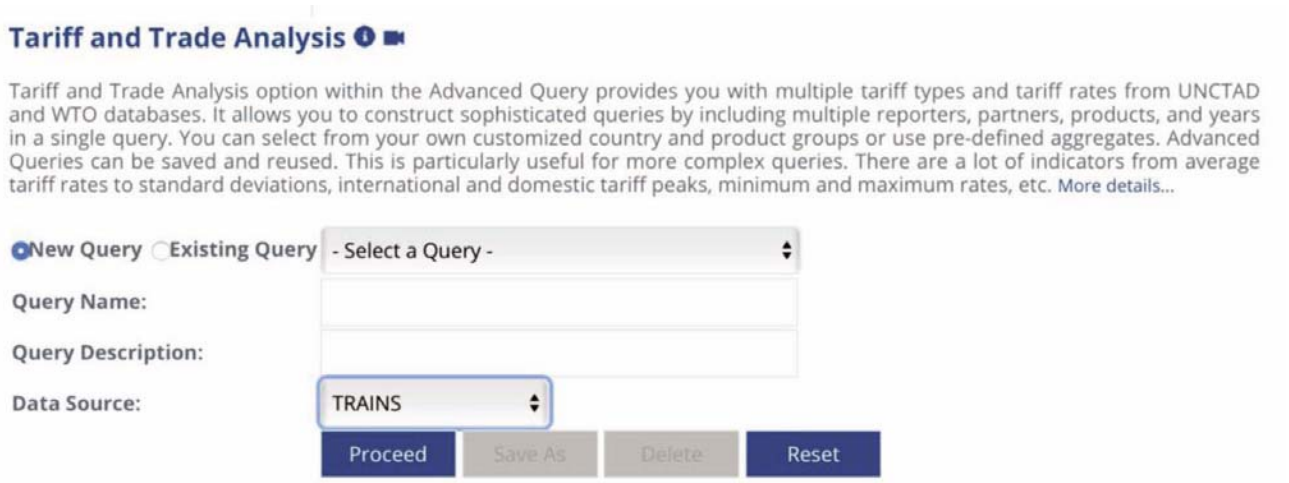
This report should be considered as a living document to be updated as the United Nations ESCAP, ECA and ECLAC, together with the EUI, and it is expected to continue updating and improving the methodology and data collection, based on feedback received from a wide range of stakeholders on this initial version. Support to member States in implementing the RDTII 2.0 guideline to evaluate and achieve evidence-based policy design and adjustments will be provided upon request, in collaboration with interested international and other organizations.

Annexes

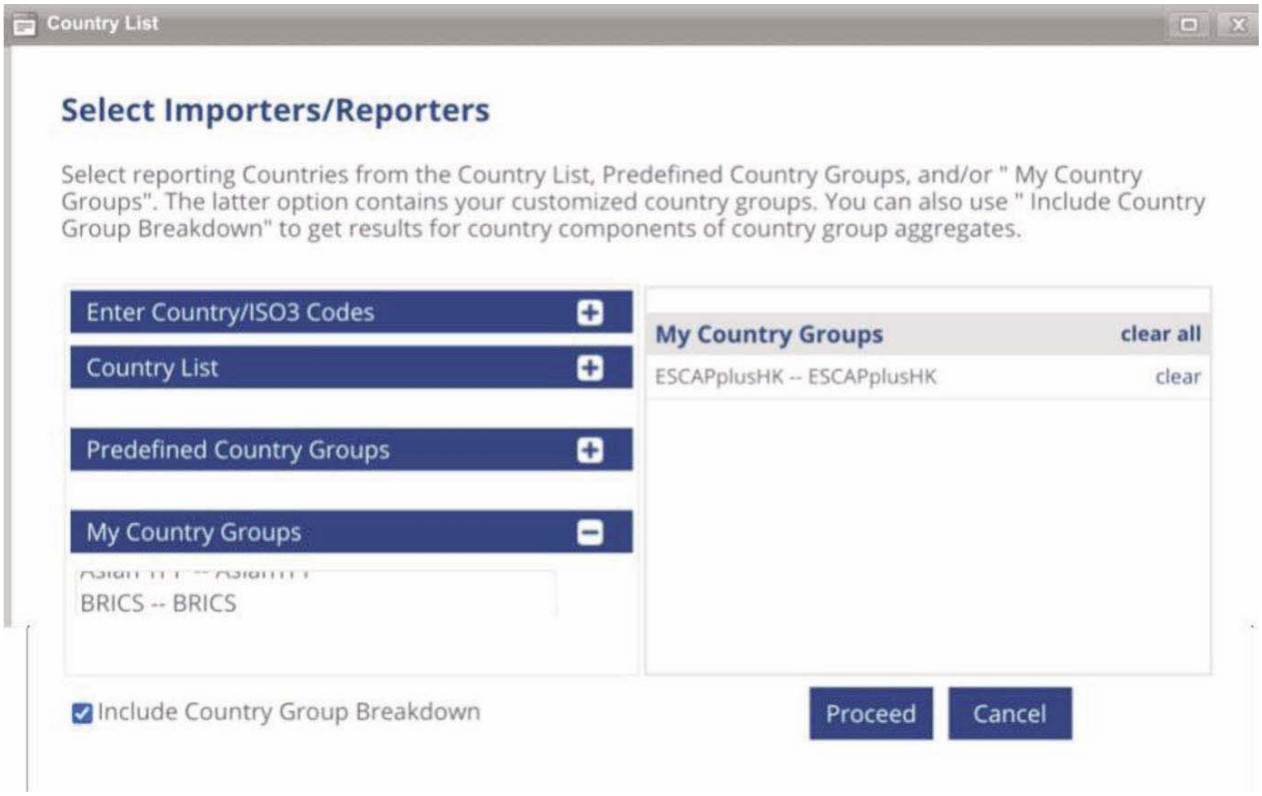
Annex I. Step-by-step guide to create data for indicators 1.1 and 1.2

1. Log in to WITS and go to 'Tariff and Trade Analysis.'

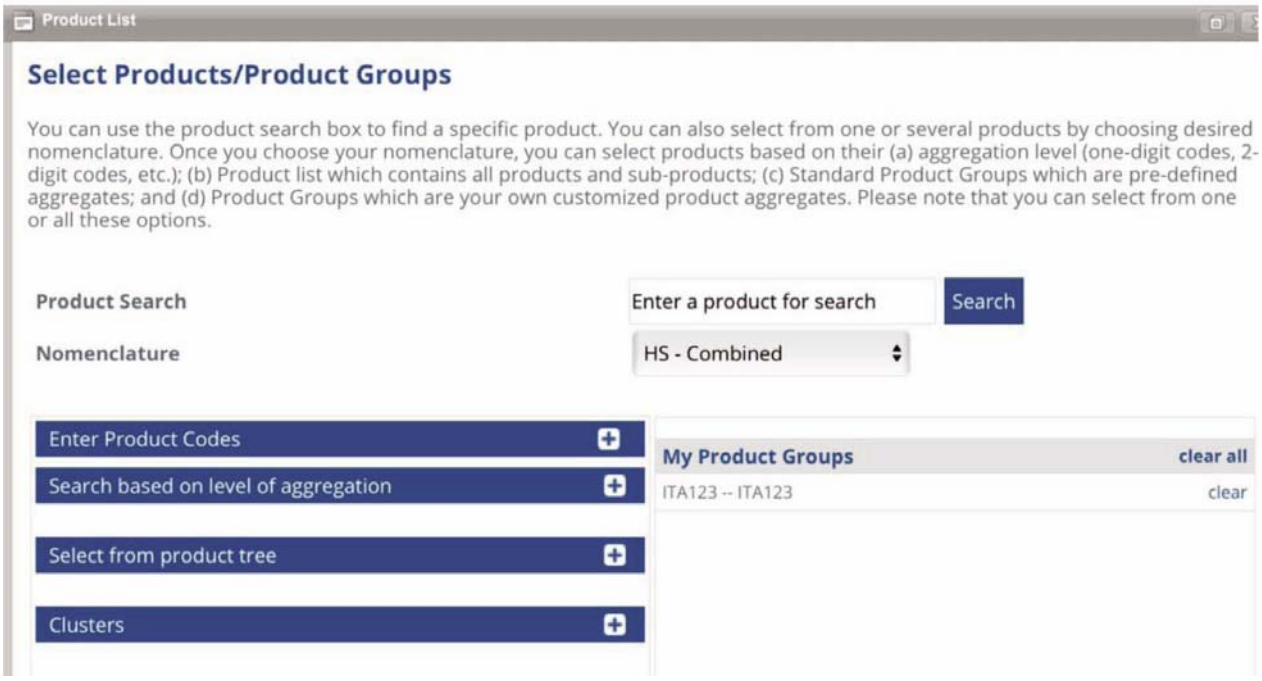
2. Add a name and description. Select 'TRAINS' as the data source.



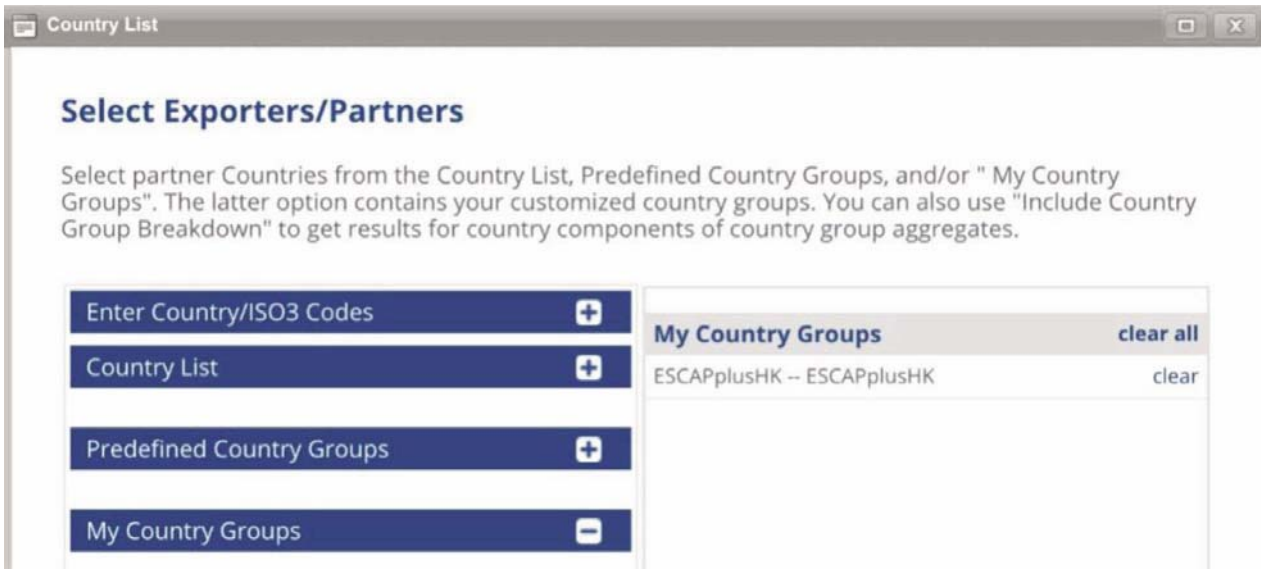
3. As importers, select the economy of interest or select all-ESCAP economy as an economy group and select 'Include economy group breakdown.'



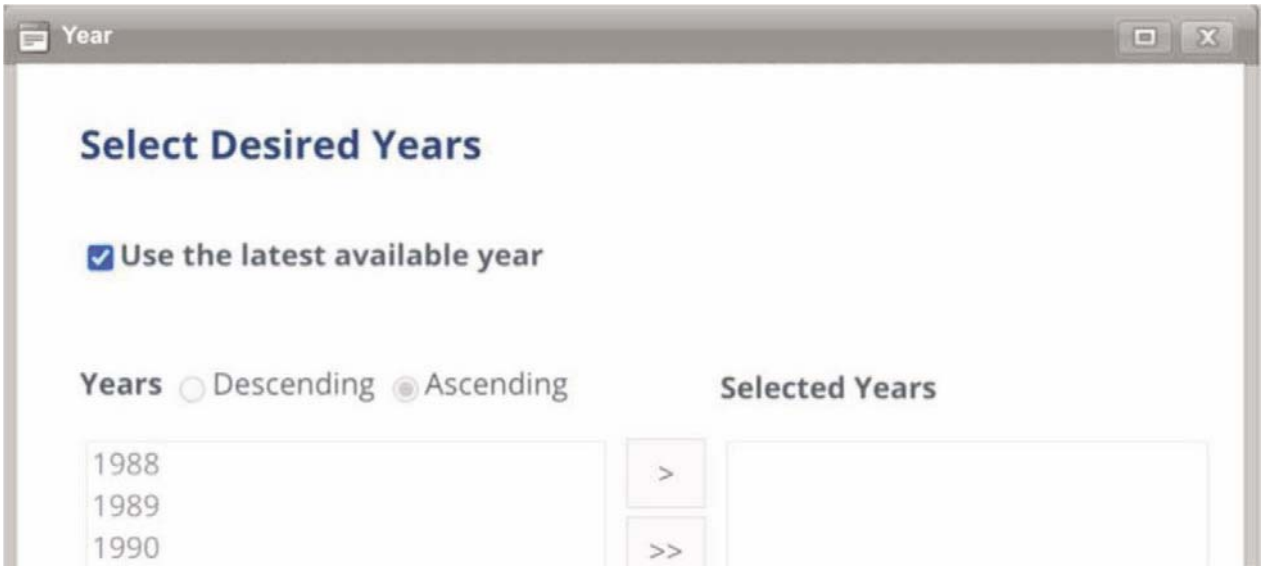
4. Select 'HS – Combined' nomenclature and select products.



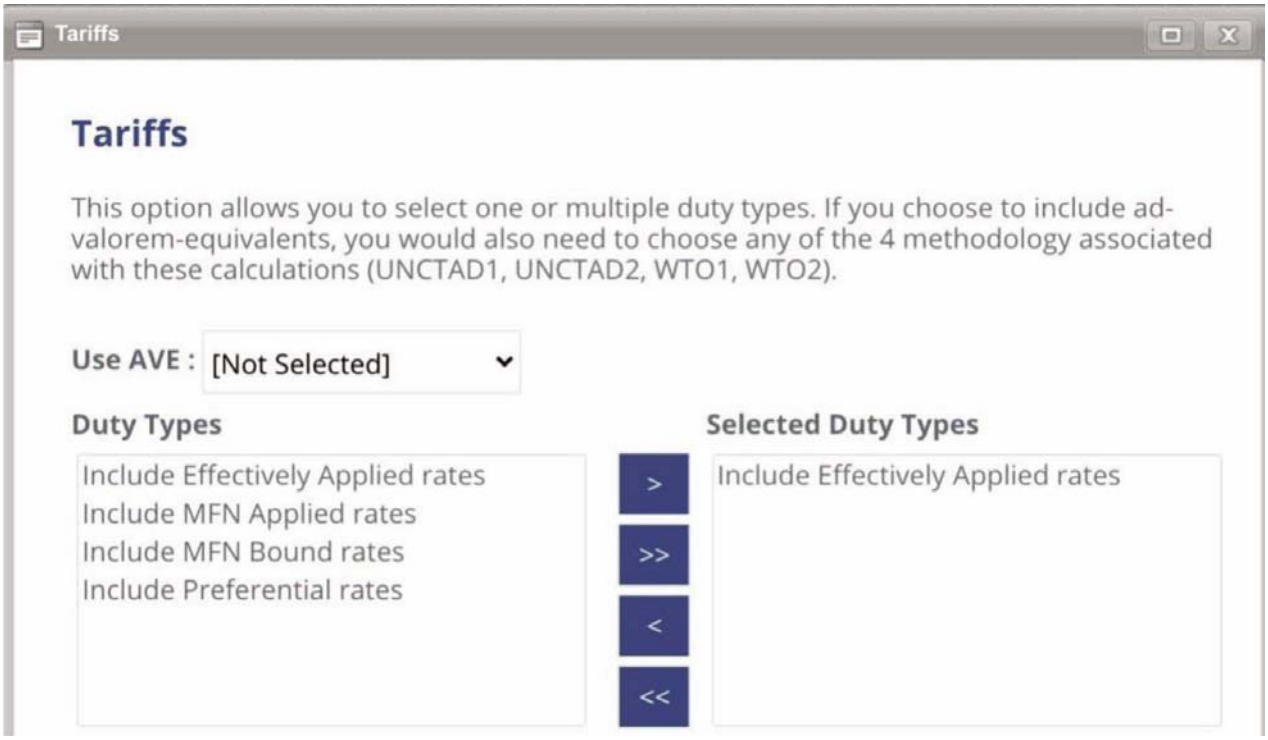
5. For exporters, select economies.



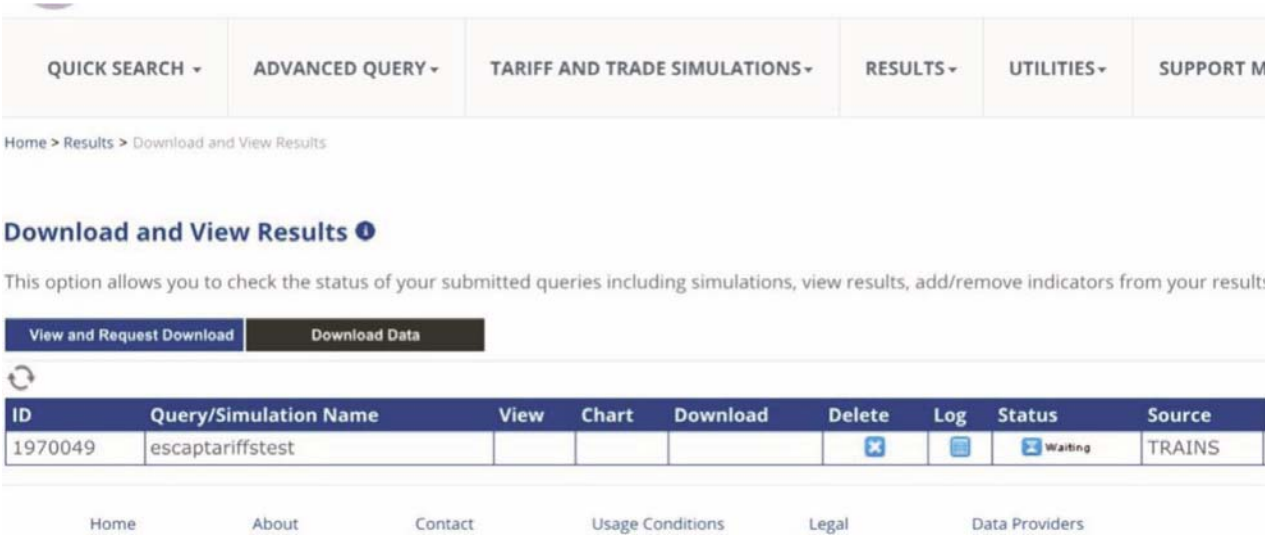
6. For year, select the latest year available.



7. As tariff, select ‘Include effectively applied rates.’

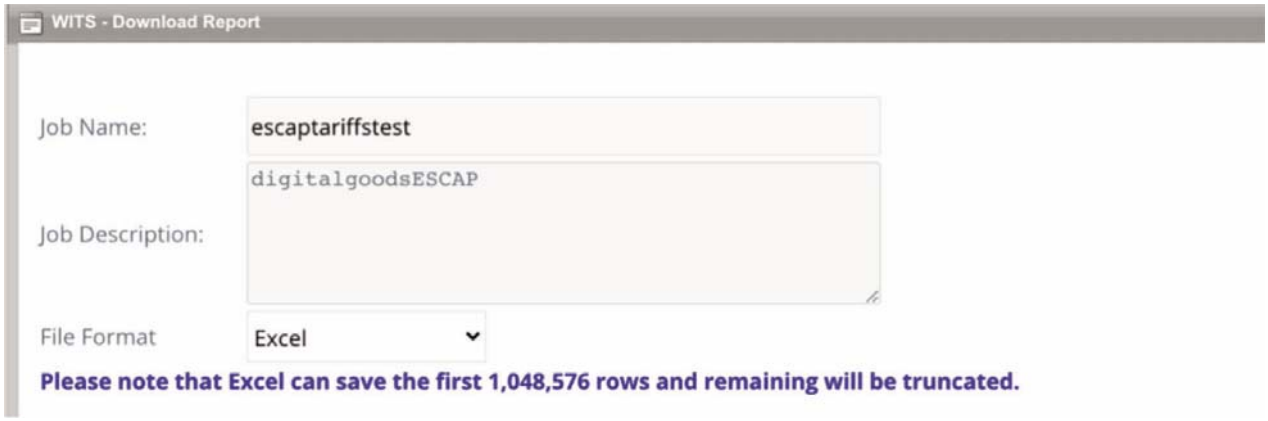


8. You will be automatically redirected to the ‘Download and View Results’ page and will need to wait until the status says ‘completed.’



9. Click ‘Download.’

10. Select ‘excel.’



11. Select also ‘Nbr of Free Lines’ (number of free lines) and then click ‘download.’

12. You will be automatically redirected to the ‘Download and View Results’ page and will need to wait until the status says ‘completed’ and then click ‘Save.’ to further download the result.

Annex II. ITA I, ITA II and ITA III products

The list of products covered under the WTO ITA I, ITA II and ITA III according to the Declaration on the Expansion of Trade in Information Technology Products,[44] and proposed products expansion by the Information Technology and Innovation Foundation (ITIF).

Lists of ITA I and ITA II

Attachment A provides the lists of the HS 2007 subheadings. The partially covered subheadings are identified with the symbol "ex".

Attachment A

Item	HS 2007	ex	Product Description
001	350691	ex	Optically clear free-film adhesives and optically clear curable liquid adhesives of a type used solely or principally for the manufacture of flat panel displays or touch-sensitive screen panels.
002	370130		Other plates and film, with any side exceeding 255 mm.
003	370199		Other.
004	370590		Other.
005	370790		Other.
006	390799	ex	Thermoplastic liquid crystal aromatic polyester copolymers.
007	841459	ex	Fans of a kind used solely or principally for cooling microprocessors, telecommunication apparatus, automatic data processing machines or units of automatic data processing machines.
008	841950	ex	Heat exchange units made of fluoropolymers and with inlet and outlet tube bores with inside diameters measuring 3 cm or less.
009	842010	ex	Roll laminators of a kind used solely or principally for the manufacture of printed circuit substrates or printed circuits.
010	842129	ex	Liquid filtering or purifying machinery and apparatus made of fluoropolymers and with filter or purifier membrane thickness not exceeding 140 microns.
011	842139	ex	Filtering or purifying machinery and apparatus for gases, with stainless-steel housing, and with inlet and outlet tube bores with inside diameters not exceeding 1.3 cm.
012	842199	ex	Parts of filtering or purifying machinery and apparatus for liquids, made of fluoropolymers and with filter or purifier membrane thickness not exceeding 140 microns; parts of filtering or purifying machinery and apparatus for gases, with stainless steel housing, and with inlet and outlet tube bores with inside diameters not exceeding 1.3 cm.

[44] Available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN15/25.pdf&Open=True

Item	HS 2007	ex	Product Description
013	842320	ex	Scales for continuous weighing of goods on conveyors using electronic means for gauging weights.
014	842330	ex	Constant weight scales and scales for discharging a predetermined weight of material into a bag or container, including hopper scales, using electronic means for gauging weight.
015	842381	ex	Other weighing machinery, having a maximum weighing capacity not exceeding 30 kg using electronic means for gauging weight.
016	842382	ex	Other weighing machinery, having a maximum weighing capacity exceeding 30 kg but not exceeding 5,000 kg using electronic means for gauging weight, excluding machines for weighing motor vehicles.
017	842389	ex	Other weighing machinery, having a maximum weighing capacity exceeding 5,000 kg using electronic means for gauging weight.
018	842390	ex	Parts of weighing machinery using electronic means for gauging weight, excluding parts of machines for weighing motor vehicles.
019	842489	ex	Mechanical appliances for projecting, dispersing or spraying of a kind used solely or principally for the manufacture of printed circuits or printed circuit assemblies.
020	842490	ex	Parts of mechanical appliances for projecting, dispersing or spraying of a kind used solely or principally for the manufacture of printed circuits or printed circuit assemblies.
021	844230		Machinery, apparatus and equipment.
022	844240		Parts of the foregoing machinery, apparatus or equipment.
023	844250		Plates, cylinders and other printing components; plates, cylinders and lithographic stones, prepared for printing purposes (for example, planed, grained or polished).
024	844331		Machines which perform two or more of the functions of printing, copying or facsimile transmission, capable of connecting to an automatic data processing machine or to a network.
025	844332		Other, capable of connecting to an automatic data processing machine or to a network.
026	844339		Other.
027	844391		Parts and accessories of printing machinery used for printing by means of plates, cylinders and other printing components of heading 84.42.
028	844399		Other.
029	845610	ex	Machine tools operated by laser or other light or photon beam processes of a kind used solely or principally for the manufacture of printed circuits, printed circuit assemblies, parts of heading 8517, or parts of automatic data processing machines.

Item	HS 2007	ex	Product Description
030	846693	ex	Parts and accessories of machine tools operated by laser or other light or photon beam processes of a kind used solely or principally for the manufacture of printed circuits, printed circuit assemblies, parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of machine-tools operated by ultrasonic processes of a kind used solely or principally for the manufacture of printed circuits, printed circuit assemblies, parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of machining centres of a kind used solely or principally for the manufacture of parts of heading 8517, or parts of automatic data processing machines; Parts and accessories of machining centres of a kind used solely or principally for the manufacture of parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of numerically controlled (other lathes) of a kind used solely or principally for the manufacture of parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of numerically controlled (other drilling) of a kind used solely or principally for the manufacture of parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of numerically controlled (other milling machines) of a kind used solely or principally for the manufacture of parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of sawing or cutting-off machines of a kind used solely or principally for the manufacture of parts of heading 8517 or parts of automatic data processing machines; Parts and accessories of machine-tools operated by electro-discharge processes of a kind used solely or principally for the manufacture of printed circuits, printed circuit assemblies, parts of heading 8517 or parts of automatic data processing machines
031	847210		Duplicating machines.
032	847290		Other.
033	847310		Parts and accessories of the machines of heading 8469.
034	847340		Parts and accessories of the machines of heading 8472.
035	847521		Machines for making optical fibres and preforms thereof.
036	847590	ex	Parts of machines of subheading 847521.
037	847689	ex	Money-changing machines.
038	847690	ex	Parts of money-changing machines.
039	847989	ex	Automated electronic component placement machines of a kind used solely or principally for the manufacture of printed circuit assemblies.
040	847990	ex	Parts of automated electronic component placement machines of a kind used solely or principally for the manufacture of printed circuit assemblies.
041	848610		Machines and apparatus for the manufacture of boules or wafers.
042	848620		Machines and apparatus for the manufacture of semiconductor devices or of electronic integrated circuits.

Item	HS 2007	ex	Product Description
043	848630		Machines and apparatus for the manufacture of flat panel displays.
044	848640		Machines and apparatus specified in Note 9(C) to this chapter.
045	848690		Parts and accessories.
046	850440		Static converters.
047	850450		Other inductors.
048	850490		Parts.
049	850590	ex	Electromagnets of a kind used solely or principally for magnetic resonance imaging apparatus other than electromagnets of heading 90.18.
050	851430	ex	Other furnaces and ovens of a kind used solely or principally for the manufacture of printed circuits or printed circuit assemblies.
051	851490	ex	Parts of other furnaces and ovens of a kind used solely or principally for the manufacture of printed circuits or printed circuit assemblies.
052	851519	ex	Other wave soldering machines of a kind used solely or principally for the manufacture of printed circuit assemblies.
053	851590	ex	Parts of other wave soldering machines of a kind used solely or principally for the manufacture of printed circuit assemblies.
054	851761		Base stations.
055	851762		Machines for the reception, conversion and transmission or regeneration of voice, images or other data, including switching and routing apparatus.
056	851769		Other.
057	851770		Parts.
058	851810		Microphones and microphone stands.
059	851821		Single loudspeakers, mounted in their enclosures.
060	851822		Multiple loudspeakers, mounted in the same enclosure.
061	851829		Other.
062	851830		Headphones and earphones, whether or not combined with a microphone, and sets consisting of a microphone and one or more loudspeakers.
063	851840		Audio-frequency electric amplifiers.
064	851850		Electric sound amplifier sets.
065	851890		Parts.
066	851981		Using magnetic, optical or semiconductor media.
067	851989		Other.
068	852110		Magnetic tape-type.
069	852190		Other.

Item	HS 2007	ex	Product Description
070	852290		Other.
071	852321		Cards incorporating a magnetic stripe.
072	852329		Other.
073	852340		Optical media.
074	852351		Solid-state non-volatile storage devices.
075	852352		“Smart cards”.
076	852359		Other.
077	852380		Other.
078	852550		Transmission apparatus.
079	852560		Transmission apparatus incorporating reception apparatus.
080	852580		Television cameras, digital cameras and video camera recorders.
081	852610		Radar apparatus.
082	852691		Radio navigational aid apparatus.
083	852692		Radio remote control apparatus.
084	852712		Pocket-size radio cassette-players.
085	852713		Other apparatus combined with sound recording or reproducing apparatus.
086	852719		Other.
087	852721	ex	Radio-broadcast receivers not capable of operating without an external source of power, of a kind used in motor vehicles, combined with sound recording or reproducing apparatus capable of receiving and decoding digital radio data system signals.
088	852729		Other.
089	852791		Combined with sound recording or reproducing apparatus.
090	852792		Not combined with sound recording or reproducing apparatus but combined with a clock.
091	852799		Other.
092	852849		Other.
093	852871		Not designed to incorporate a video display or screen.
094	852910		Aerials and aerial reflectors of all kinds; parts suitable for use therewith.
095	852990	ex	Other, excluding organic light emitting diode modules and organic light emitting diode panels for the apparatus of subheadings 8528.72 or 8528.73.
096	853180	ex	Other apparatus excluding doorbells, chimes, buzzers and similar.

Item	HS 2007	ex	Product Description
097	853190		Parts.
098	853630		Other apparatus for protecting electrical circuits.
099	853650		Other switches
100	853690	ex	Other apparatus, excluding battery clamp of a kind used for motor vehicles of heading 8702, 8703, 8704, or (8711).
101	(853810)		Boards, panels, consoles, desks, cabinets and other bases for the goods of heading 8537, not equipped with their apparatus.
102	853939	ex	Cold-cathode fluorescent lamps (CCFLs) for backlighting of flat panel displays.
103	854231		Processors and controllers, whether or not combined with memories, converters, logic circuits, amplifiers, clock and timing circuits, or other Circuits.
104	854232		Memories.
105	854233		Amplifiers.
106	854239		Other.
107	854290		Parts.
108	854320		Signal generators.
109	854330	ex	Electroplating and electrolysis machines of a kind used solely or principally for the manufacture of printed circuits.
110	854370	ex	Articles specifically designed for connection to telegraphic or telephonic apparatus or instruments or to telegraphic or telephonic networks.
111	854370	ex	Microwave amplifiers.
112	854370	ex	Cordless infrared remote-control devices for video game consoles.
113	854370	ex	Digital flight-data recorders.
114	854370	ex	Portable battery-operated electronic reader for recording and reproducing text, still image or audio file.
115	854370	ex	Digital signal processing apparatus capable of connecting to a wired or wireless network for the mixing of sound.
116	854390		Parts.
117	880260	ex	Telecommunications satellites.
118	880390	ex	Parts of telecommunication satellites.
119	880521		Air combat simulators and parts thereof.
120	880529		Other.
121	900120		Sheets and plates of polarising material.
122	900190		Other.

Item	HS 2007	ex	Product Description
123	900219		Other.
124	900220		Filters
125	900290		Other.
126	901050		Other apparatus and equipment for photographic (including cinematographic) laboratories; negatoscopes.
127	901060		Projection screens.
128	901090	ex	Parts and accessories of articles of subheadings 901050 and 901060.
129	901110		Stereoscopic microscopes.
130	901180		Other microscopes.
131	901190		Parts and accessories.
132	901210		Microscopes other than optical microscopes; diffraction apparatus.
133	901290		Parts and accessories.
134	901310	ex	Telescopes designed to form parts of machines, appliances, instruments or apparatus of this Chapter or Section XVI.
135	901320		Lasers, other than laser diodes.
136	901390	ex	Parts and accessories, other than for telescopic sights for fitting on arms or for periscopes.
137	901410		Direction finding compasses.
138	901420		Instruments and appliances for aeronautical or space navigation (other than compasses).
139	901480		Other instruments and appliances.
140	901490		Parts and accessories.
141	901510		Rangefinders.
142	901520		Theodolites and tachymeters (tacheometers).
143	901540		Photogrammetrical surveying instruments and appliances.
144	901580		Other instruments and appliances.
145	901590		Parts and accessories.
146	901811		Electro-cardiographs.
147	901812		Ultrasonic scanning apparatus.
148	901813		Magnetic resonance imaging apparatus.
149	901819		Other.
150	901820		Ultra-violet or infra-red ray apparatus.
151	901850		Other ophthalmic instruments and appliances.

Item	HS 2007	ex	Product Description
152	901890	ex	Electro-surgical or electro-medical instruments and appliances, and parts and accessories thereof.
153	902150		Pacemakers for stimulating heart muscles, excluding parts and accessories.
154	902190		Other.
155	902212		Computed tomography apparatus.
156	902213		Other, for dental uses.
157	902214		Other, for medical, surgical or veterinary uses.
158	902219		For other uses.
159	902221		For medical, surgical, dental or veterinary uses.
160	902229		For other uses.
161	902230		X-ray tubes.
162	902290	ex	Parts and accessories of apparatus based on the use of X-rays.
163	902300		Instruments, apparatus and models, designed for demonstrational purposes (for example, in education or exhibitions), unsuitable for other uses.
164	902410		Machines and appliances for testing metals.
165	902480		Other machines and appliances.
166	902490		Parts and accessories.
167	902519		Other.
168	902590		Parts and accessories.
169	902710		Gas or smoke analysis apparatus.
170	902780		Other instruments and apparatus.
171	902790		Microtomes; parts and accessories.
172	902830		Electricity meters.
173	902890		Parts and accessories.
174	903010		Instruments and apparatus for measuring or detecting ionising radiations.
175	903020		Oscilloscopes and oscillographs.
176	903031		Multimeters without a recording device.
177	903032		Multimeters with a recording device.
178	903033	ex	Other, without a recording device, excluding resistance measuring Instruments.
179	903039		Other, with a recording device.
180	903084		Other, with a recording device.

Item	HS 2007	ex	Product Description
181	903089		Other.
182	903090		Parts and accessories.
183	903110		Machines for balancing mechanical parts.
184	903149		Other.
185	903180		Other instruments, appliances and machines.
186	903190		Parts and accessories.
187	903220		Manostats.
188	903281		Hydraulic or pneumatic.
189	950410		Video games of a kind used with a television receiver.
190	950430	ex	Other games, operated by coins, banknotes, bank cards, token, or by any other means of payment, other than automatic bowling equipment and games of chance that immediately return a monetary award.
191	950490	ex	Video game consoles and machines, other than those of subheading 950430.

Source: WTO Ministerial Declaration on the Expansion of Trade in Information Technology Products.
Available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN15/25.pdf&Open=True

Attachment B

Attachment B provides the lists of specific products to be covered by the Declaration, whether they are classified in the HS 2007. The partially covered subheadings are identified with the symbol "ex".

Item	Product description
192	**Multi-component integrated circuits (MCOs):** a combination of one or more monolithic, hybrid, or multi-chip integrated circuits with at least one of the following components: silicon-based sensors, actuators, oscillators, resonators or combinations thereof, or components performing the functions of articles classifiable under heading 8532, 8533, 8541, or inductors classifiable under heading 8504, formed for all intents and purposes indivisibly into a single body like an integrated circuit, as a component of a kind used for assembly onto a printed circuit board (PCB) or other carrier, through the connecting of pins, leads, balls, lands, bumps or pads. For the purpose of this definition the following expressions mean: 1. "Components" may be discrete, manufactured independently then assembled onto the rest of the MCO, or integrated into other components. 2. "Silicon based" means built on a silicon substrate, or made of silicon materials, or manufactured onto integrated circuit die. 3(a). "Silicon based sensors" consist of microelectronic or mechanical structures that are created in the mass or on the surface of a semiconductor, and that have the function of detecting physical or chemical quantities and transducing these into electric signals, caused by resulting variations in electric properties or displacement of a mechanical structure. "Physical or chemical quantities" relates to real world phenomena, such as pressure, acoustic waves, acceleration, vibration, movement, orientation, strain, magnetic field strength, electric field strength, light, radioactivity, humidity, flow, chemicals concentration etc. 3(b). "Silicon based actuators" consist of microelectronic and mechanical structures that are created in mass or on the surface of a semiconductor and that have the function of converting electrical signals into physical movement. 3(c). "Silicon based resonators" are components that consist of microelectronic or mechanical structures that are created in mass or on the surface of a semiconductor and have the function of generating a mechanical or electrical oscillation of a predefined frequency that depends on the physical geometry of these structures in response to an external input. 3(d). "Silicon based oscillators" are active components that consist of microelectronic or mechanical structures that are created in mass or on the surface of a semiconductor and that have the function of generating a mechanical or electrical oscillation of a predefined frequency that depends on the physical geometry of these structures.
193	**Light-Emitting Diode (LED) Backlights modules,** which are lighting sources that consist of one or more LEDs, and one or more connectors, and are mounted on a printed circuit or other similar substrate, and other passive components, whether or not combined with optical components or protective diodes, and used as backlights illumination for liquid crystal displays (LCDs).

Item	Product description
194	**Light-Emitting Diode (LED) Backlights modules,** which are lighting sources that consist of one or more LEDs, and one or more connectors and are mounted on a printed circuit or other similar substrate, and other passive components, whether or not combined with optical components or protective diodes, and used as backlights illumination for liquid crystal displays (LCDs).
195	**Ink cartridges** (with or without an integrated print head) for insertion into apparatus of HS subheadings 844331, 844332 or 844339, and incorporating mechanical or electrical components; thermoplastic or electrostatic toner cartridges (with or without moving parts) for insertion into apparatus of HS subheadings 844331, 844332 or 844339; solid ink inengineered shapes for insertion into apparatus of HS subheadings 844331, 844332 or 844339.
196	**Printed matter** which grants the right to access, install, reproduce or otherwise use software (including games), data, Internet content (including in-game or in-application content) or services, or telecommunications services (including mobile services).[28]
197	**Self-adhesive circular polishing pads** of a kind used for the manufacture of semiconductor Wafers.
198	**Boxes, cases, crates and similar articles,** of plastic, specially shaped or fitted for the conveyance or packing of semiconductor wafers, masks, or reticles of subheading 392310 or 848690.
199	**Vacuum pumps** of a kind used solely or principally for the manufacture of semiconductors or flat panel displays.
200	**Plasma cleaner machines** that remove organic contaminants from electron microscopy specimens and specimen holders.
201	**Portable interactive electronic education devices** primarily designed for children.

Source: WTO Ministerial Declaration on the Expansion of Trade in Information Technology Products. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN15/25.pdf&Open=True

List of ITA III (proposed expansion)

HS 2017 code included in the proposed second expansion of the WTO's Information Technology Agreement.

ITA-3 Proposed Expansion							
281290	630790	847989	852580	900490	392119	843139	850780
282739	680530	847990	852692	900691	392190	844332	850790
284590	681510	848071	852721	900699	392310	844399	851130
285000	690390	848180	852791	900850	392321	845011	851180
285390	690911	848410	852852	901090	392329	845620	851190
292090	690919	850110	852859	901110	392610	845650	851410
292111	700719	850131	852862	901180	392690	845690	851430
293139	701710	850132	852869	901190	401699	847130	851679
293190	702000	850133	852871	901210	420212	847141	851712
321590	731815	850134	852872	901290	420222	847149	851762
340220	741521	850161	852873	901320	420291	847150	851769
340290	741533	850162	852990	901380	420292	847180	851770
340590	760611	850163	853180	901390	420299	847330	851810
370110	761699	850164	853530	901814	420500	847480	851822
370242	820320	850431	853540	901819	481940	847529	851829
370244	820540	850440	853590	901890	482190	847590	851890
370710	830220	850450	853610	901910	540771	847780	852341
380110	830249	850490	853641	902580	560311	847790	852349
382499	841330	850511	853669	902610	591140	847950	852351
390230	841410	850519	853670	902620	854420	903289	880220
390290	841490	850520	853710	902690	854430	903290	880230
390469	841810	850590	853720	902710	854442	903300	880240
390599	841869	850610	853890	902720	854449	910291	880260
390730	841919	850640	853950	902750	854519	910511	900211
390740	841989	850650	853990	902780	854690	910591	900219
391000	842119	850660	854079	902790	854710	911320	960830
391732	842121	850680	854089	902810	854720	911390	962000
391740	842129	850720	854150	902820	854790	940310	
391910	842139	850730	854310	903033	854890	940320	
391990	842191	850740	854370	903120	870830	940390	
392049	842199	850750	854411	903141	880211	940540	
392099	842890	850760	854419	903180	880212	950691	

Source: Information Technology and Innovation Foundation, Appendix D, available at https://www2.itif.org/2021-ITA-3.pdf

References

Anant, V., Donchak, L., Kaplan, J., and Soller, H. (2020). The Consumer-Data Opportunity and the Privacy Imperative. McKinsey and Company, 27 April. Available https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Asian Business Law Institute (ABLI) (2020). Transferring Personal Data in Asia: A Path to Legal Certainty and Regional Convergence. Singapore: ABLI. Available at https://abli.asia/abli-publications/transferring-personal-data-in-asia-a-path-to-legal-certainty-and-regional-convergence-2/

Association of Southeast Asian Nations (ASEAN) (2012). ASEAN Sectoral Mutual Recognition Arrangement for Electrical and Electronic Equipment. ASEAN, 18 July. Available at https://asean.org/asean-sectoral-mutual-recognition-arrangement-for-electrical-and-electronic-equipment/

European Commission (2018a). What Constitutes Data Processing? Available at https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en#:~:text=Examples%20of%20processing%20include%3A,-staff%20management%20and&text=shredding%20documents%20containing%20personal%20data,video%20recording%20(CCTV)

_____(2018b). What is a Data Protection Impact Assessment (DPIA) Required? Available at https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en#:~:text=A%20DPIA%20is%20required%20at,areas%20on%20a%20large%20scale

Ezell and Dascoli (2021). Information Technology and Innovation Foundation (ITIF). Available at https://itif.org/publications/2021/09/16/how-an-information-technology-agreement-3-0-would-bolster-global-economic-growth-and-opportunity/

Federal Communications Commission (FCC) (2016). Equipment Authorization APEC TEL MRA. Available at https://www.fcc.gov/general/equipment-authorization-apec-mra

Ferracane, M.F. (2017). Restrictions on Cross-Border Data Flows: A Taxonomy. European Centre for International Political Economy (ECIPE) Working Paper, No.1/2017, 21 December. Brussel: ECIPE. Available at https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf

Ferracane, M.F., Lee-Makiyama, H. and van der Marel, E. (2019). Digital Trade Restrictiveness Index. European Centre for International Political Economy (ECIPE): Brussels. Available at https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Frosio, G. (2020). *Oxford Handbook of Online Intermediary Liability*. Oxford University Press. Available at https://global.oup.com/academic/product/oxford-handbook-of-online-intermediary-liability-9780198837138?cc=th&lang=en&

3GPP (2008). About 3GPP. Available at https://www.3gpp.org/about-3gpp

GSMA (2019). Infrastructure sharing: An overview, 18 June. Available at https://www.gsma.com/futurenetworks/wiki/infrastructure-sharing-an-overview/

Hayes, S. (2021). EMC vs. EMI Testing: What's the Difference, and What Do I Need to Consider? Element Materials Technology, 21 December. Available at https://www.element.com/nucleus/2017/whats-the-difference-emc-vs-emi

Houben, R. and Snyers, A. (2018). Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion. Directorate-General for Internal Policies of the Union (European Parliament), 6 September. Available at https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

International Chamber of Commerce (ICC) (2016). ICC Policy Statement on Global Baseline De Minimis Value Thresholds. ICC, 11 November. Available at https://iccwbo.org/news-publications/policies-reports/icc-policy-statement-on-global-baseline-de-minimis-value-thresholds-2015/

IMF, UNCTAD, OECD, and WTO. (2023). Handbook on Measuring Digital Trade: Second Edition. Available at https://www.imf.org/en/Publications/Books/Issues/2023/08/17/Handbook-on-Measuring-Digital-Trade-Second-edition-537466

Keller, D. (2018). A Glossary of Internet Content Blocking Tools. The Center for Internet and Society (CIS), Sandford Law School, 29 January. Available at http://cyberlaw.stanford.edu/blog/2018/01/glossary-internet-content-blocking-tools

Ketels, C. and Bhattacharya, A. (2019). Global Trade Goes Digital. Boston Consulting Group (BCG), 12 August. Available at https://www.bcg.com/publications/2019/global-trade-goes-digital

Organisation for Economic Co-operation and Development (OECD) (2011). Internet Intermediaries, Definitions, Economic Models and Role in the Value Chain. Chapter 1, pp.19-36. In *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. Paris: OECD Publishing. Available at https://read.oecd-ilibrary.org/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives/internet-intermediaries_9789264115644-4-en#page1

_____(2018). Trade and Cross-border Data Flows. Working Party of the Trade Committee, Trade and Agriculture Directorate, 21 December. Available at https://one.oecd.org/document/TAD/TC/WP(2018)19/FINAL/En/pdf

_____(2022). Recommendation of the Council Concerning Guidelines for Cryptography Policy. OECD Legal Instruments. Available at https://legalinstruments.oecd.org/public/doc/115/115.en.pdf

Pacific Economic Cooperation Council (PECC) and Access Partnership (2021). Primer and Economic Integration Issues Posed by the Digital Economy. PECC Signature Project on the Digital Economy, 8 November. Singapore: PECC. Available at https://www.pecc.org/resources/digital-economy/2705-pecc-signature-project-primer-on-economic-integration-issues-posed-by-the-digital-economy/file

Rucz, M. and Kloosterboer, S. (2020). Data Retention Revisited. European Digital Rights (EDRi), 28 September. Available at https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

Singapore, Infocomm Media Development Authority (2020). Data Protection Assured, Trust Is Now Certified. Available at https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Success-Stories-130820.pdf

_____(2024). Data Protection Trustmark Certification. Available at https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification

Sobol M. (2016). Exceptions to copyright in Russia and the “fair use” doctrine. European Audiovisual Observatory. Available at https://rm.coe.int/1680783347

United Nations (1991). Provisional Central Product Classification. Statistical Papers, series M, No.77. Available at https://www.wto.org/english/tratop_e/serv_e/cpc_provisional_complete_e.pdf

United Nations Commission on International Trade Law (UNCITRAL) (2018a). UNCITRAL Model Law on Electronic Commerce 1996 with Additional Article 5bis as Adopted in 1998. Available at https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

_____(2018b). UNCITRAL Model Law on Electronic Signatures (2001). Available at https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

_____(2018c). United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005). Available at https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications

United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) (2017). Digital and Virtual Currencies for Sustainable Development. ESCAP Trade, Investment and Innovation, Policy Brief, 13 November. Bangkok: ESCAP. Available at https://www.unescap.org/resources/digital-and-virtual-currencies-sustainable-development

World Customs Organization (WCO) (2016). What is the Harmonized System (HS)? Available at http://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx

World Trade Organization (WTO) (2000). Agreement on Government Procurement. Available at https://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm

_____(2001). Information Technology Agreement: An Explanation. Available at https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm