

Regional Digital Trade Integration Index (Version 1): A Guide



ESCAP
MOVING FORWARD TOGETHER



ECA



UNITED NATIONS

ECLAC

Regional Digital Trade Integration Index (Version 1): A Guide

20 June 2022



ECA



UNITED NATIONS

ECLAC

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 composed of 54 member States and is playing a dual role as a regional arm of the United Nations and a key component of the African institutional landscape. The thematic areas of ECA focus on macroeconomic policy; regional integration and trade; social development; natural resources; innovation and technology; and gender and governance. To enhance its impact, ECA places particular emphasis on: collecting up-to-date and original regional statistics in order to base its policy research and advocacy on clear, objective evidence; promoting policy consensus; providing meaningful capacity development; and providing advisory services to African Governments, intergovernmental organizations and institutions in key thematic fields. It also formulates and promotes development assistance programmes and acts as the executive agency for relevant operational projects. 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 coordinating 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.

Copyright © United Nations 2022

All rights reserved

For further information on this publication, please contact: escap-tiid@un.org.

ECLAC Symbol: LC/TS.2022/100

Disclaimer

The views expressed in this publication are those of the authors and do not necessarily reflect the views of the United Nations Economic and Social Commission of Asia and the Pacific (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.

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 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, ESCAP, with significant inputs from ESCAP consultants, Martina Francesca Ferracane, Yohan Nah and Natnicha Sutthivana. Simon Mevel, Geoffroy Guepie and Jason Mc Cormack provided comments and inputs from the ECA region, while Johan Mulder provided inputs from ECLAC region. The publication also benefited from comments received from national focal points and experts in the economies covered under this initiative.

The report also draws inputs from economy-level data collected by ESCAP consultants, including Aditi Pandey, Archana Subramanian, Ayushi Singh, Fandi Achmad, Juan F. Rodrigo Lopez, Kshitiz Dahal, LE Thu Ha, Natnicha Sutthivana, Runqiu Du, Said Jafarli, Sariyya Bunyatova, and Yohan Nah. Francis Mark Quimba and Sylwyn C. Calizo from the Philippine Institute for Development Studies contributed inputs related to the Philippines. Wannarat Charoensri provided technical assistance in the formatting and layout of the publication.

Preface

The regional digital trade integration index (RDTII) results from cooperation among several United Nations Regional Commissions. Its development was initiated at ESCAP in 2020 as part of developing a broader Digital and Sustainable Regional Integration Index (DigiSRII) under a joint UN Development Account project on measuring regional integration led by ECA and jointly implemented with ESCWA. Implementation of RDTII was pilot-tested in Asia and the Pacific and subsequently extended to several economies in the ECA and ECLAC regions.

This guide is based on the methodology and indicators of RDTII Version 1.0. It provides essential explanations of the structure and rationale of RDTII 1.0 and guidance on data collection and sources. It is expected to give a guideline to those involved in collecting regulatory data to analyze the digital trade regulatory environment based on the RDTII 1.0 framework. It is useful also for those who will use the index and related indicators for policy analysis and drafting. The RDTII framework, a multi-dimensional cross-economy index of digital trade regulatory integration, is expected to require continuous adjustments as the challenges and policy trade-offs associated with fast-growing digital trade and the global digital economy are better understood. As such, this guide may be considered a living document to be updated as United Nations Regional Commissions and other partners work together further to improve the index and the data collection process.

Contents

Acknowledgements	iv
Preface	v
List of boxes.....	vii
List of figures.....	vii
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): Indicating the regulatory costs of doing regional business digitally	3
Chapter 2 RDTII framework	6
Scoring methodology.....	7
Sources of regulatory measures	8
Chapter 3 RDTII pillars.....	10
Pillar 1. Tariffs and trade defence measures.....	11
Pillar 2. Public procurement	15
Pillar 3. Restrictions on foreign investment	20
Pillar 4. Intellectual property rights policies.....	24
Pillar 5. Telecommunications infrastructure and competition.....	29
Pillar 6. Cross-border data policies.....	33
Pillar 7. Domestic data policies	40
Pillar 8. Internet intermediary liability and content access.....	46
Pillar 9. Non-technical NTMs.....	51
Pillar 10. Technical standards and related procedures.....	54
Pillar 11. Online sales and transactions	60
Chapter 4 Concluding remarks	65
Annex I. Step-by-step guide to create data for indicators 1.1 and 1.2.....	67
Annex II. ITA I and ITA II products.....	72
References.....	80

List of boxes

Box 1. The RDTII framework in brief.....	4
Box 2. The Agreement on Government Procurement (GPA).....	18
Box 3. The Patent Cooperation Treaty (PCT)	25
Box 4. International encryption standards for import encryption methods.....	58
Box 5. Relationship among the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures and the United Nations Convention on the Use of Electronic Communications.....	64

List of figures

Figure 1. Simplification and interoperability of digital trade rules	2
Figure 2. RDTII's methodology	7
Figure 3. Republic of Korea's regulatory measures.....	9
Figure 4. Tension among different policy objectives in Pillar 1	11
Figure 5. Pillar's indicators and the weights	14
Figure 6. Tension among different policy objectives in Pillar 2	15
Figure 7. Pillar 2's indicators and the weights	19
Figure 8. Tension among different policy objectives in Pillar 3	20
Figure 9. Pillar 3's Indicators and the weights.....	23
Figure 10. Balance in policy objectives in Pillar 4.....	24
Figure 11. Pillar 4's indicators and the weights	28
Figure 12. Balance in policy objectives in Pillar 5.....	29
Figure 13. Pillar 5's indicators and the weights	32
Figure 14. Balance in policy objectives in Pillar 6.....	33
Figure 15. Conditions of local storage, processing and infrastructure	36
Figure 16. Conditions of consent, evaluation and approval	37
Figure 17. Pillar 6's indicators and the weights	39
Figure 18. Balance in different policy objectives in Pillar 7	40
Figure 19. Pillar 7's indicators and the weights	45
Figure 20. Balance in different policy objectives in Pillar 8	46
Figure 21. Pillar 8's indicators and the weights	50
Figure 22. Tension among different policy objectives in Pillar 9	51
Figure 23. Pillar 9's indicators and the weights	53
Figure 24. Balance in different policy objectives in Pillar 10	54
Figure 25. Pillar 10's indicators and the weights	59
Figure 26. Balance in different policy objectives in Pillar 11	60
Figure 27. Pillar 11's indicators and the weights	64

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
BORCA	Botswana Communications Regulatory Authority
B2B	business to business
CABs	Conformity Assessment Bodies
CBPR	Cross-Border Privacy Rules system
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CPC	Central Product Classification
DigiSRII	Digital and Sustainable Regional Integration Index
DNS	domain name system
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSI	digital line subscribers
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
EU	European Union
FIPS	Federal Information Processing Standard
FSS	Federal Security Service
GCI	Global Competitiveness Index
GDPR	General Data Protection Regulation
GTA	Global Trade Alert
3GPP	3rd Generation Partnership Protection
HS	Harmonised System
ICC	International Chamber of Commerce
ICLG	International Comparative legal Guides
ICPs	internet content providers
ICT	information and communication technology
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IP	intellectual property
IPRs	intellectual property rights
ISO	International Organization for Standardization
ISPs	internet service providers

IT	information technology
ITA	International Telecommunication Union
I-TIP	Integrated Trade Intelligence Portal
LCRs	local content requirements
MFN	most-favoured nation
MLEC	Model Law on Electronic Commerce
MLÉS	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
PTA	Preferential trade agreement
RDTII	Regional Digital Trade Integration Index
RM	Malaysian ringgit
SDoC	supplier declaration of conformity
SDR	special drawing rights
SMEs	small medium-sized enterprises
SOEs	state-owned enterprises
SORM	System for Operational Investigative Measures
STRI	Services Trade Restrictiveness Index
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
TRAINS	Trade Analysis Information System
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
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



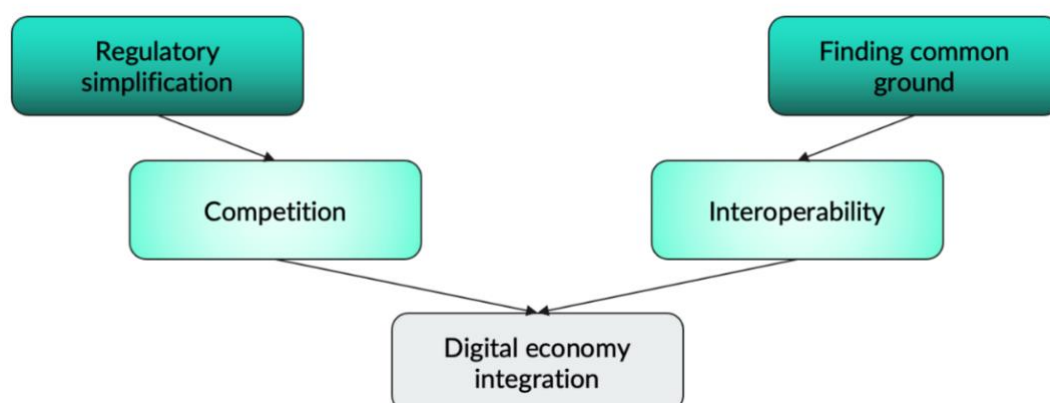
Background

Digital trade is defined as “digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms and Governments” (OECD, 2019). 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, when there is a regulation in place or without it, 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. By reducing regulatory compliance costs, the regulatory simplification is supposed to encourage competition. The competition will bring innovation to different sectors. 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): Indicating the regulatory costs of doing regional business digitally

The Regional Digital Trade Integration Index (RDTII) seeks to provide a comprehensive view of the state of play of various regulatory measures affecting digital trade integration beyond those that might be considered trade barriers. The RDTII framework has been used in the digital-trade regulatory analysis in the Asia-Pacific, Africa and Latin America and the Caribbean regions. It identifies 11 policy areas, or “Pillars”, to evaluate the regulatory environment affecting digital trade businesses (box 1). 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 business’. In addition, the RDTII framework considers that enhancing regional integration through more digital trade between the Asia-Pacific economies requires promoting the interoperability of digital-trade regulatory approaches, reducing the costs of regulatory compliance, and promoting intraregional trade in goods and services that are important to the development of the digital economy, such as ICT goods and ICT 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, the RDTII 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 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 framework aims to support policymakers in making informed policy decisions by bringing the fact that more regulations typically increase compliance costs to support. Such costs tend to be fixed costs, which have disproportionate effects on small firms compared to large firms and may prevent entry by a firm of all sizes in small markets.

Box 1. The RDTII framework in brief



The overall RDTII is a composite index integrating the scores of 11 pillars using a simple average method. Each RDTII pillar score is the weighted average of scores at the indicator level. 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 that are provided online** relative to those provided offline.
- **Absence of certain international agreements, legislation, or legal mechanism** considered of significant importance for interoperability across jurisdictions.

The RDTII framework considers that enhancing regional integration through more digital trade between economies requires finding common ground between different digital-trade regulatory approaches as well as reducing policy restrictions that affect intraregional trade in goods and services that are important to the development of digital economy, such as ICT goods, digital 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.

Pillar 1 covers **tariffs and trade defence** measures that limit trade in ICT goods within the considered UN region.

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

Pillar 3 covers **restrictions on foreign 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 **IPR policies** and the balance between protecting individual exclusive rights to intellectual property and fostering innovation.

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

Pillar 6 considers policies on **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 and restrictions on content access**, 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 captures **non-technical 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 considered region.

Pillar 10 focuses on **technical standards and related procedures**. This pillar considers the 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.

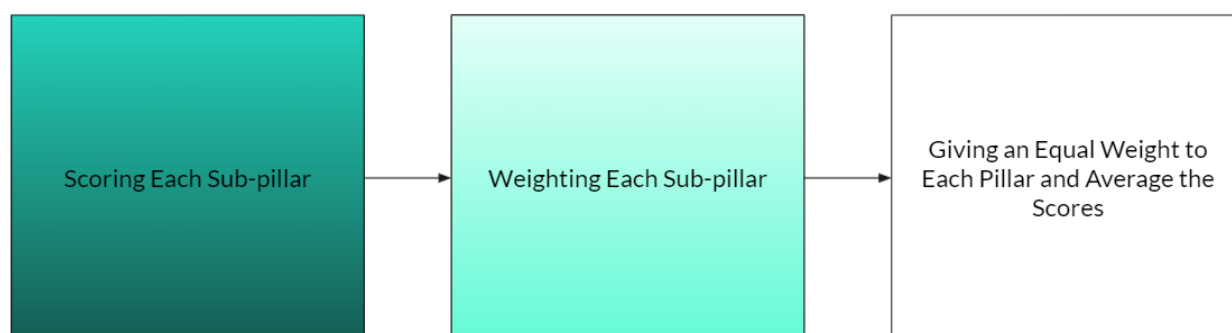
Pillar 11 captures a broad spectrum of policies that affect **online sales and transactions**, including regulations on delivery, advertising, online payment, domain names, as well as legal recognition for electronic contracts, electronic signatures and the existence of relevant consumer protection laws.

Chapter 2 RDTII framework



The RDTII framework identifies 11 policy domains that shape the digital-trade regulatory environment. Each Pillar has 3-5 policy indicators as proxies for the regulatory environment in respective policy area. Calculating a RDTII score of an economy requires three steps, as shown in figure 2: (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 score to the economy.

Figure 2. RDTII's methodology



Scoring methodology

RDTII aims to indicate the interoperability of regulatory regimes in the regions in terms of trade and compliance costs. For this, the score in each indicator runs from ‘0’ (simplified) to ‘1’ (heavily regulated). A score which is greater than ‘0’ indicates one of the following.

First, a measure implies **a differential treatment** between domestic and foreign providers of ICT goods, digital goods or online services despite being in the same or similar circumstances. For example:

- A measure that does not allow public procurement bidding unless a bidding entity is a national of the regulating economy. 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 it serves to ensure cybersecurity, it discourages firms from submitting a bid due to the fear of technology transfer or additional costs for reconfiguration.

Third, an economy **fails to adopt** a certain international agreement, legislation or legal mechanism considered to be of significant importance in the development of digital trade. For example:

- Being a signatory to the WTO Information Technology Agreement;
- Being a signatory to the WTO Agreement on Government Procurement;

- The doctrine of fair use;
- Legislation for data protection;
- Safe-harbour provision for Internet intermediaries;
- Legislation for electronic transactions and signatures.

Weighting indicators

To generate a score from a Pillar, the RDTII takes an unweighted approach across the 11 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 M. F. 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 scores

While the RDTII applies unequal weights to the indicators within each pillar, it applies an equal weight on each pillar to produce a final RDTII score for an economy. The composite RDTII runs from 0 (simplified) to 1 (heavily regulated).¹

Sources of regulatory measures

Researchers should look at the official gazette of laws, regulations and other measures to find relevant information for each indicator. Secondary sources such as official guidelines, official government reports and publications, and legal reviews serve only to guide researchers' attention to the primary sources. Examples of useful secondary sources are shown Pillar-by-Pillar below.

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

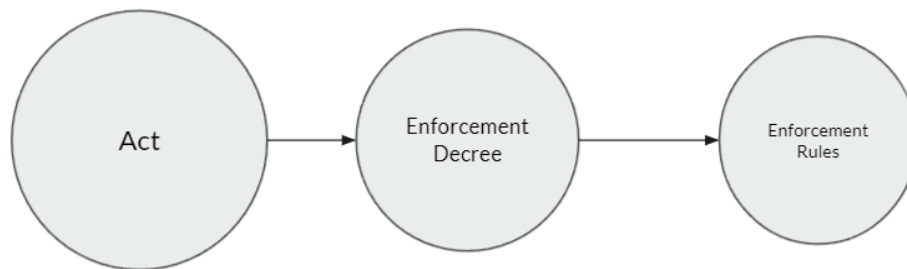
First, there may be a gap between what the law says (*de jure*) and how that law applies (*de facto*). Usually, this results from (a) considerable discretion in decision-making and implementation of regulation, and (b) a lack of transparency on institutional structures.

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 3. The Enforcement

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.

Decrees and Rules, which are promulgated by administrative agencies, spell out in detail what Acts mandate, which are enacted by the legislature.

Figure 3. Republic of Korea's 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 restrictions, the researchers should cite the Public Procurement Act or other regulations governing public procurement in the economy as reference.

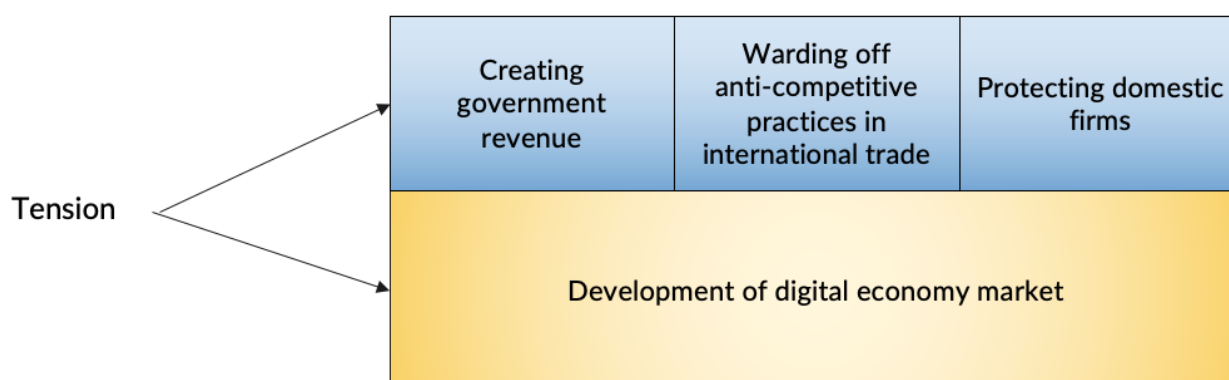
Chapter 3 RDTII pillars



Pillar 1. Tariffs and trade defence measures

Pillar 1 covers tariffs and trade defence measures applied to intraregional imports of ICT goods.² As figure 4 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 the 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 4. Tension among different policy objectives in Pillar 1



Pillar 1 measures consider the following areas:

- Effectively applied tariffs on ICT-related goods (in weighted average) imported from other economies within the considered United Nations region;
- Coverage ratio of zero-tariff lines on ICT goods from other economies within the considered United Nations region;
- The status of being a signatory to the WTO Information Technology Agreement (ITA) of 1996 (ITA I) and its expansion in 2015 (ITA II); and
- Anti-dumping, countervailing duties and safeguards on ICT-related goods imported by other economies within the considered United Nations region.

² ICT products or ICT goods are 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 1.0 results are based on the list of ICT products found in Lee-Makiyama, 2011.

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 products 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.

Coverage rate of zero-tariffs on ICT goods imported from other economies within the considered United Nations region

The second indicator is the coverage rate of zero-tariffs that apply to ICT goods 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 coverage ratio duty tariffs are greater than 30%, the score will be truncated to '0' if its duty-free coverage rate is above 30%. 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.

³ An effectively applied tariff is defined by WITS as the lowest available tariff. If a preferential tariff exists, it will be used as the effectively applied tariff. Otherwise, the MFN applied tariff will be used. 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.

The status of being a signatory to the WTO 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 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 the 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 the 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 the 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 are the 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](#) is also a useful secondary source. The secondary source should only serve to guide researchers to the primary sources.

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. 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 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.'

⁴ The ITA concessions are included in the participants' WTO schedules of concessions, 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.

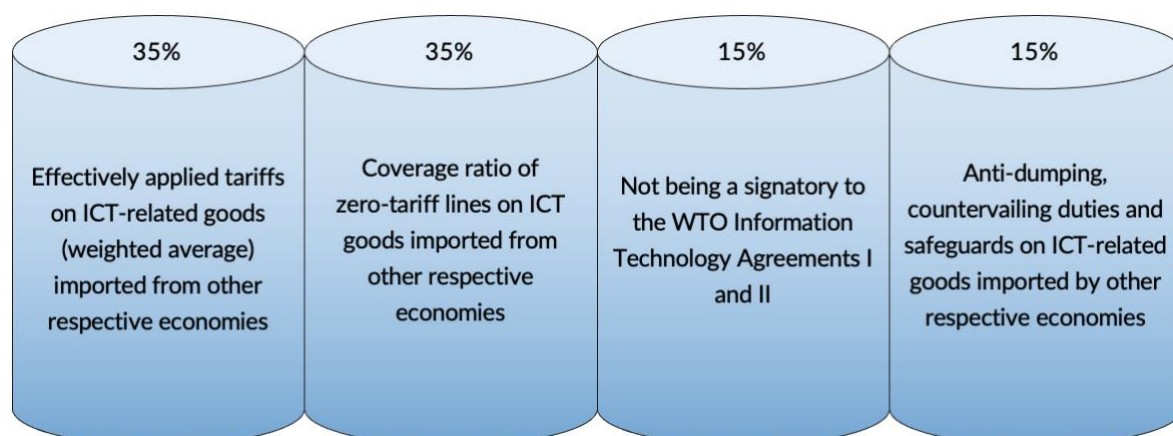
⁵ For the list of products covered under the WTO's ITA I and ITA II, please see Annex II.

For sources, find WTO members' [anti-dumping notifications](#) under the agreement on implementation of Article VI of GATT 1994 (“G/ADP/N/1/...”) or the most recent official gazette of a relevant national ministry. Useful secondary sources include [the Integrated Trade Intelligence Portal \(ITIP\)](#) and [the Global Trade Alert \(GTA\) database](#). The secondary sources should serve only to guide researchers' attention to the primary sources.

The weights of each indicator

As shown in figure 5, weight rates of 35%, 35%, 15% and 15% are given to the indicators, respectively. The first two indicators are given a greater weight equally than the last two indicators. 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. Furthermore, the fact that an economy is not a member of the 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 lesser weight.

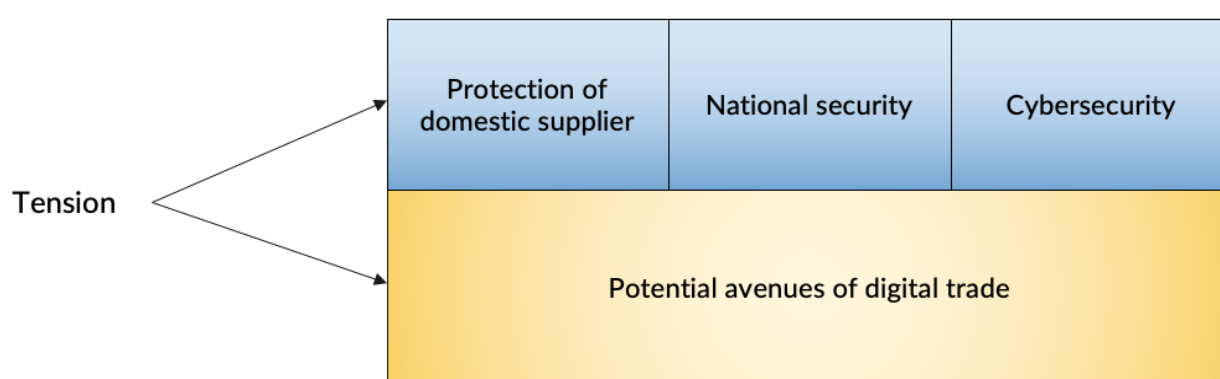
Figure 5. Pillar's indicators and the weights



Pillar 2. Public procurement

Pillar 2 covers measures on public procurement related to ICT goods and online services. There is tension among different policy objectives in procurement policies, as shown in figure 6. It looks into 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 *per se* potential avenues of digital trade.

Figure 6. 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:

- Exclusion of foreign firms from public procurement, including ICT goods and online services;
- Requirements on source codes, encryption and trade secrets;
- Other limitations on participation in procurement bidding; and
- Being a signatory to 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).

Exclusion of foreign firms from public procurement, including ICT goods and online services

This indicator covers measures that may exclude foreign enterprises from public procurement. 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.

An economy receives a score of ‘1’ if the economy excludes foreign enterprises from public procurement. The score is ‘0.5’ if there is an instance where an economy has excluded a specific (group of) foreign firm(s) from public procurement. The score is ‘0’ if such a measure does not exist.

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 its bidding.

A requirement to transfer technology or use a specific encryption standard in public procurement often stems from the interest in protecting national security. However, these kinds of requirements may prevent foreign companies from entering the domestic market because of concern about 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 Republic of Korea requires that suppliers of certain software, network and hardware equipment submit the source code of their products to pass “the Cryptographic Module Validation Process”;
- 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 ‘0.5’ if firms are required to use specific encryption to win tenders. The score is ‘1’ if there are two or more requirements to use specific encryption or if there is a requirement to surrender such trade secrets as a condition for participating in 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.

Other limitations on participation in procurement bidding

This indicator covers limitations on participation in public procurement. These limitations can take various forms: (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;
- There are local content requirements giving a 15% preference to goods produced in Rwanda and a 10% preference to bidders registered in Rwanda;
- The Nigerian Guidelines on Content Development in ICT require 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;
- 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;
- In Argentina, 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. 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 exists and there is institutional transparency.

The status of being a signatory to 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)⁶ 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 sectors (United Nations, 1991). Each party’s coverage schedule can be found at the [e-GPA Portal](#).

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 extension 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 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.

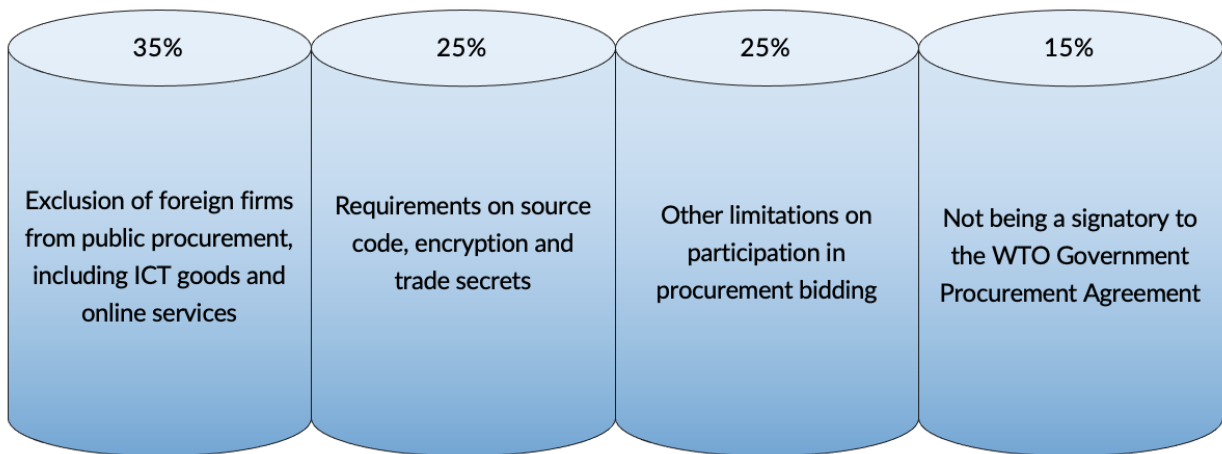
The weights of each indicator

As shown in figure 7, weights for each indicator are 35%, 25%, 25%, and 15%, respectively. The exclusion of foreign firms from procurement receives the most significant weight because it discriminates against foreign firms and *per se* bans foreign participation in public procurement. The requirements on trade secrets and other limitations on participating in procurement receive a lesser weight because they do not discriminate against foreign firms. 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

⁶ Available at https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm.

discriminates against foreign firms or adds regulatory compliance costs in procurement. Therefore, the weight of this indicator is less than the others.

Figure 7. Pillar 2's indicators and the weights

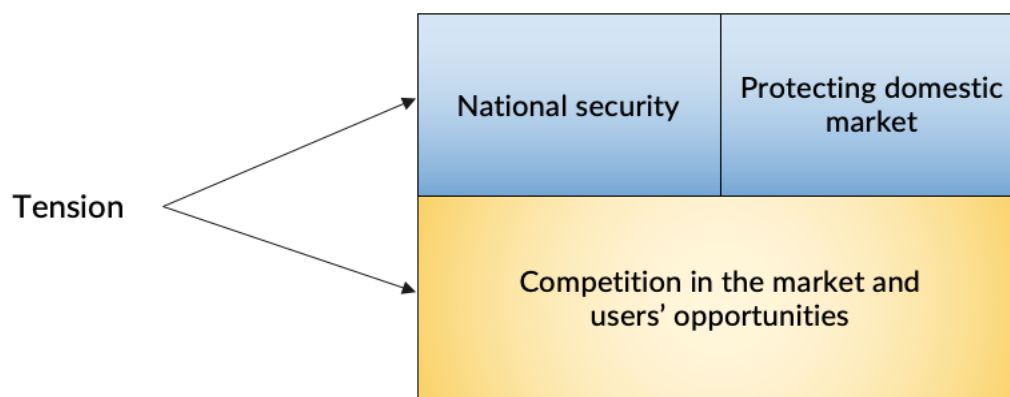


Pillar 3. Restrictions on foreign investment

Pillar 3 covers measures on foreign direct investment 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 foreign direct investment (FDI) policies may exist between the interests to protect national security and the domestic market and the need to attract FDI (figure 8). 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 8. 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:

- Maximum foreign equity shares in sectors relevant to digital trade;
- Joint-venture requirement in sectors relevant to digital trade;
- Nationality or residency requirement for board of directors or managers in sectors relevant to digital trade; and
- Screening of investment and acquisitions in sectors relevant to digital trade

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 Regulatory Database](#), and [the GTA database](#). The secondary sources should only serve to guide researchers to the primary sources.

Maximum foreign equity shares in sectors relevant to digital trade

This indicator concerns maximum foreign equity shares in sectors related to digital trade. 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 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 requirement in sectors relevant to digital trade

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 the 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 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,
- The Liberian 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.’

Nationality or residency requirement for 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.⁷

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.’

Screening of investment and acquisitions in sectors relevant to digital trade

This indicator asks whether an economy has adopted any screening mechanism for foreign investment or mergers and acquisitions 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 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. Examples of the screening mechanisms include:

- 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;
- Cambodia requires foreign investors to register with a governmental agency, which reserves the right to deny the issuance of “conditional registration certificates” for investment projects “related to national interest or environmental sensitivity.”
- 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 competitiveness of the economy;
- The Republic of Korea declines a foreign investment if there is clear evidence that this investment poses a threat to national security or public interest;
- 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 to qualify for private investment incentives;
- The Uganda Investment Code Act stipulates certain screening measures for local and foreign investors intending to invest in information technology.

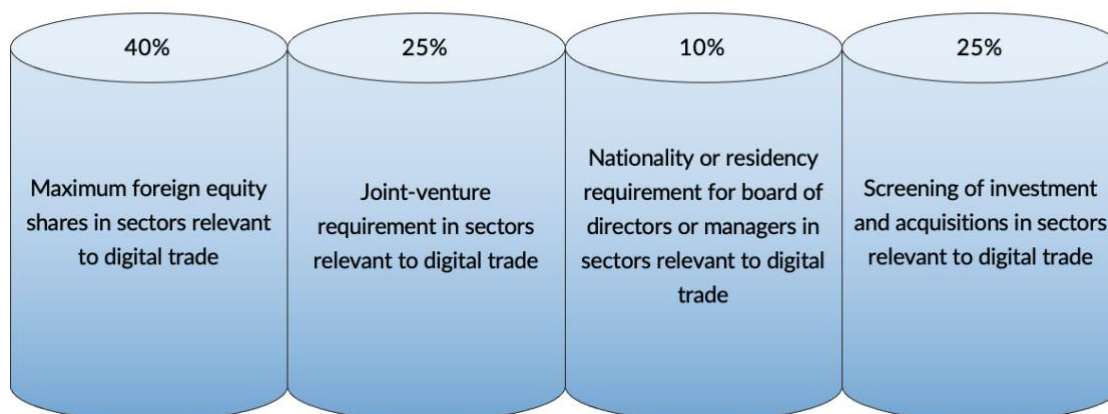
⁷ Residency or nationality requirements that apply only to officers who are not directors or managers do not count under this sub-pillar.

For any screening mechanism, the score is ‘0.5.’ If two or more mechanisms exist, the score is ‘1.’ If there is no screening mechanism, the score is ‘0.’

The weights for each indicator

As shown in figure 9, the weights are 40%, 25%, 10% and 25%, respectively. The greatest weight, 40%, is given to the first indicator since the numerical limitations on foreign ownership flatly discriminate against foreign investors and directly block foreign investment. The second indicator – a joint-venture requirement – is given the weight of 25% because, 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 fourth indicator – screening of investment and acquisitions – is given the same weight of 25% since, while it discourages foreign investors due to the time and cost involved in the screening process and less predictability and certainty, it does not block *per se* foreign ownership. The third indicator – nationality or residency requirements for directors or managers – is given the least weight, 10%, since the degree to which these requirements discourage foreign investment is relatively limited.

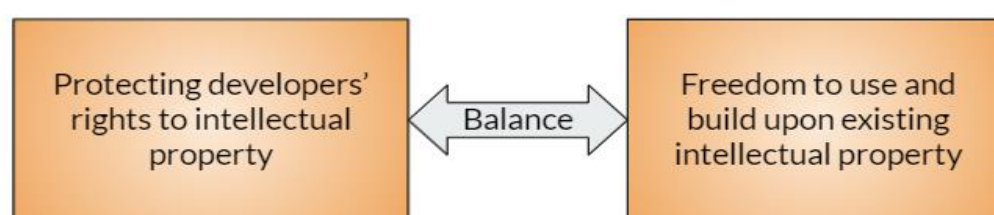
Figure 9. Pillar 3's Indicators and the weights



Pillar 4. Intellectual property rights policies

Pillar 4 deals with intellectual property rights (IPRs). 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 10, 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 10. Balance in policy objectives in Pillar 4



The Pillar 4 comprises the following indicators:

- Restrictions on application process for patents;
- Presence of copyright exceptions;
- Inadequate enforcement of copyright;
- Mandatory disclosure of trade secrets such as source code and algorithms; and
- IPR environment (Global Competitiveness Index (GCI), Pillar 1.15).

Restrictions on application process for patents

This indicator covers restrictions on the application process for local and international patents. Specifically, these restrictions refer to the lack of membership in the WIPO Patent Cooperation Treaty (PCT) (box 3) and domestic restrictions. Goods enabled by digital technologies often entail patents. The PCT 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.

Domestic restrictions such as high filing fees, requirements to appoint a local patent agent, and different terms of patent protection that apply to foreign applicants rather than to domestic applicants discourage or discriminate against foreign patent applicants.⁸ Some economies impose a requirement to file a patent locally 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

⁸ Different terms of patent protection that apply 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.

applicant must file a patent application in China first. This provision is applicable to all Chinese entities, including a subsidiary of a foreign company which is also considered a Chinese entity. Requirements like this could discourage businesses, either domestic or foreign firms in the market, from participating in digital trade.

Moreover, the domestic restrictions could cause a rejection of the patent application in a discretionary manner, considering as the measures directly hinder the patent application process. For example, in Lao PDR, a patent or petty patent shall be refused if contrary to the culture, social orders, and security. With regards to this case, the rejection of patents based on the ground of public policy is uncertain and burdens the applicants who wish to seek a patent registration in such economy.

For scoring, the score is ‘0.5’ if an economy is not the PCT membership and/or for a requirement on the application process that merely discourages trade. The score is ‘1’ if there exists a requirement that directly hinders the patent, or if there are two or more requirements that may discourage trade. The score is ‘0’ if there is no restriction. [The PCT Applicant’s Guide \(national phase\)](#) is a useful secondary source. The secondary sources should only serve to guide researchers to the primary sources.

Box 3. The Patent Cooperation Treaty (PCT)

The PCT is an international treaty that was concluded in 1970, and now has more than 150 Contracting States. The PCT facilitates patent protection for an invention simultaneously in a large number of economies by filing 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 advantages of the PCT include the following. 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 the 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 the 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.

Presence of copyright exceptions

This indicator asks what type of copyright exceptions, if any, an economy has adopted. The exceptions allow lawful use of copyrighted works without obtaining permission or license 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 the 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, 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.

Third, some economies have an exception similar to the doctrine of fair dealing but with a wider range of permissible uses, including making changes to software and databases for the purposes of archiving the copy of software and database and de-compilation of software as in the Russian Federation.

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 has no copyright exceptions. The score is ‘0.5’ if an economy does not adopt the fair use doctrine but has other exceptions, such as the fair dealing doctrine or a three-step test. The score ‘0.5’ also includes when an economy does not adopt an explicit fair use or fair dealing regime, but the copyrights exception is implemented. The score is ‘0’ if an economy adopts fair use (or both fair use and fair dealing).

Inadequate enforcement of copyright

This indicator asks whether an economy adequately protects copyright. 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 holders.

For scoring, if an economy fails to have a legislative approach to tackle copyright piracy, the score is '1.' If an economy has the legislative framework, but 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.'

[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.

Mandatory disclosure of trade secrets such as source code and algorithms

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

- The Russian Federation can request that Internet companies hand over their encryption keys;
- China reportedly requires companies to provide source code or encryption keys to ensure the security and controllability of the information systems;
- 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.

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.

It will not get scored when the Government mandates to disclose trade secrets and takes proper measures to protect 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 product will get a score of 0.5. The score is '1' if there is more than one such measure. The score is also '1' if the requirement is comprehensive, affecting an entire sector or all sectors horizontally. If there is no such measure, the score is '0.'

IPR environment (GCI, Pillar 1.15)

This indicator gives a general overview of the IPR environment in an economy concerned. It draws upon [the Global Competitiveness Index \(GCI\)](#) score on the IPR environment (Pillar 1.15 of the GCI), which seeks business executives' opinions on the extent to which IPR is protected in their

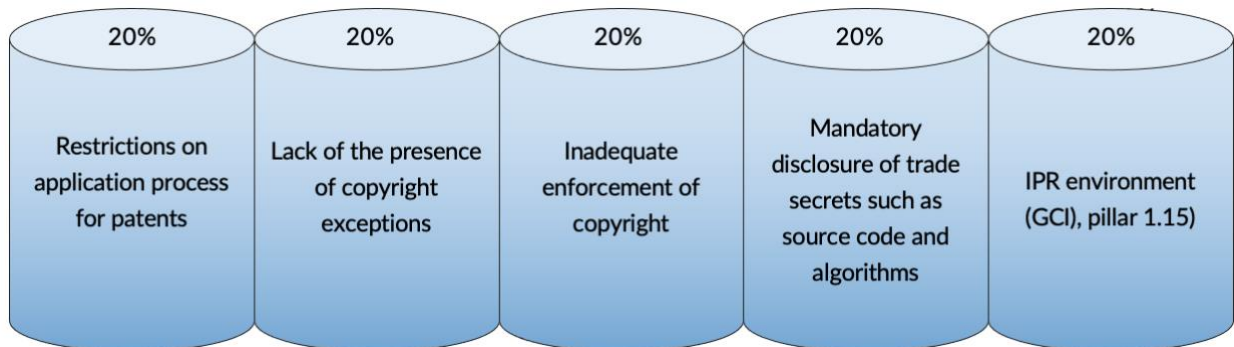
economy. To estimate the score for this entry, the indicator uses a linear function, $f(x) = 1 - (x/7)$, where x is the GCI score. The function converts the GCI score scale from 1 to 7 into a scale between 0 to 1.

The score is '0.5' for each of the measures above.

The weights for each indicator

As shown in in figure 11, each indicator is given an equal weight rate of 20%.

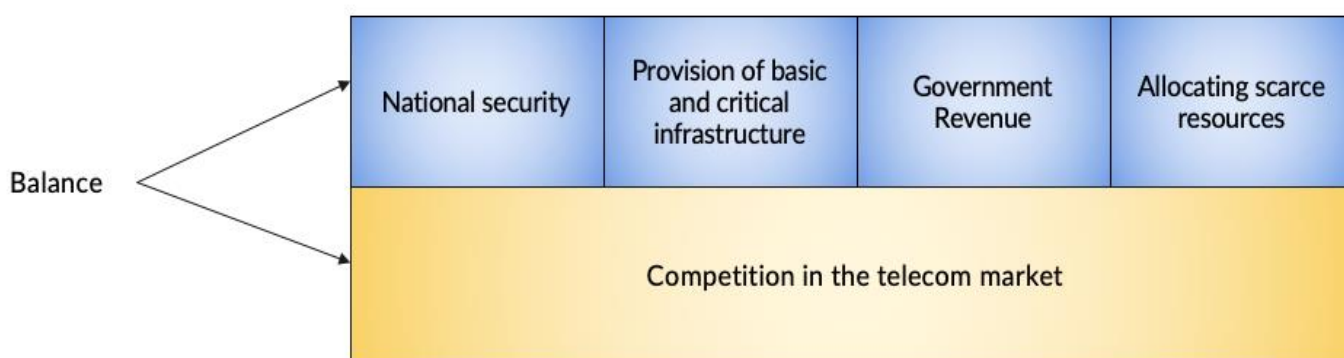
Figure 11. Pillar 4's indicators and the weights



Pillar 5. Telecommunications infrastructure 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 12, with the policy environment that is conducive to competition among domestic and foreign telecom providers.

Figure 12. Balance in policy objectives in Pillar 5



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

- Lack of liberalization of the telecommunication sector;
- Anti-competitive practices in the telecommunication sector and other measures; and
- Strict licensing requirements.

Useful secondary sources include [the Law Review](#), 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](#), and [the OECD Digital STRI database](#). The secondary sources should only serve to guide researchers to the primary sources.

Lack of liberalization of the telecommunication sector

This indicator looks at the degree to which the telecommunication-facility sector has been liberalized. There are three factors to be considered in determining whether the sector has been ‘liberalized’. First, the extent to which the telecom-facility sector has been regulated under competition rules rather than subject to a monopoly or an oligopoly; second, whether foreign ownership in telecom facilities is allowed; and third, whether access networks, or ‘the last mile,’ are owned by a dominant player in the market.⁹ Whether or not a telecommunication company is a dominant player in the market

⁹ The ‘last mile’ refers to the final section of the telecommunications networks that delivers telecommunication services to end-users. It is mostly through a wired or wireless connection. A wired connection is based on either copper or fibre-optic cables, and a wireless connection is based on radio communication. A wired connection enables data and voice transmission via the Internet, while a wireless connection enables mobile communication, Wi-Fi, Bluetooth, etc.

is determined based on the circumstances of the market, including its market share for the telecommunication facilities in the economy, whether the company is either fully or partly state-owned, and whether the company provides essential telecommunication services.

The presence of competition rules governing the telecom facilities is critical for the digital economy and trade. The lack of competition rules to prevent monopoly power over network facilities and discriminatory measures against foreign investors could undermine efficient access to ‘last mile’ or telecommunication networks essential for digital trade businesses.

The score is ‘1’ if the telecom facilities in an economy are not subject to competition rules or if foreign ownership in the facilities is not allowed. The score is ‘0.5,’ where, although the facilities are subject to competition rules, access networks are still owned by a dominant player in the market. The score is ‘0’ if there exist competition rules, foreign ownership in telecom facilities is allowed, and a dominant player does not own the majority of access networks.

Anti-competitive practices in the telecommunication sector and other measures

This indicator asks whether there are anti-competitive practices in the telecom market and other measures. Anti-competitive practices by firms include collusionary agreement, exclusive dealing, tying, predatory pricing and refusal to deal. These could take the form of, in the context of telecommunications, antitrust agreements among incumbent telecom firms, different conditions for interconnection given to companies providing equivalent services, high interconnection fees, and refusal for interconnection.

Other measures by the Government are open-ended. For example:

- Kazakhstan requires telecom carriers to purchase certain telecom equipment for the Government. It is reported that the telecommunication companies are required to purchase and install equipment related to the state’s System for Operational Investigative Measures (SORM) and to cover costs related to the database of International Mobile Equipment Identity (IMEI) codes as well as pay regular fees to the State Radio Frequency Service, which is the IMEI database operator;
- In Nigeria, it is mandatory for telecommunications equipment to undergo testing procedures in line with the procedures of the Nigerian Communication Commission, and equipment must obtain a certificate that it meets the Commission’s type approval standards before shipment into Nigeria. It is also mandatory that an end-user certificate be obtained for the supply of specific telecommunications equipment like frequency jammers equipment, satellite dishes, satellite transmitters and receivers;
- Japan exercises considerable discretion in allocating radio frequencies. Japan allocates them through the “partial auction system,” whereby the agency considers the amount of special fees submitted by the applicant based on their valuation of the spectrum, although it is not a decisive element;
- New Zealand imposes a duty on network operators to decrypt communications with the assistance of law enforcement.

Anti-competitive practices among telecom-facility providers discourage foreign as well as domestic firms from doing business in the market. This includes not only telecom services but also products and services related to digital trade. Measures on operating telecom facilities or providing telecom services, likewise, can create similar problems.

Each anticompetitive practice or restriction counts as ‘0.5.’

Strict licensing requirements

This indicator asks two questions: (a) whether there are strict licensing requirements for telecom-facility providers, network providers and telecom-service providers; and (b) whether there are discriminatory conditions that are applied to foreign companies to obtain licences for providing telecom facilities or services.

With regard to the first question, while most economies have licensing schemes in sectors relevant to telecommunication, licensing schemes in certain sectors are “strict”, in that they have the potential to block or discourage 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 some licences for the provision of broadcasting services.

Furthermore, licensing schemes that are well-established practices have some requirements (or conditions for obtaining a licence) that are “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;
- In Tanzania, holders of licences for network facilities and network services are required 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 Licence” for foreign investment in telecommunication services generally as well as sector-specific licences for wireless and wired connection;
- Kazakhstan requires telecom service providers to connect their channels to a public network controlled by a state-owned telecom company as a condition for winning a licence.

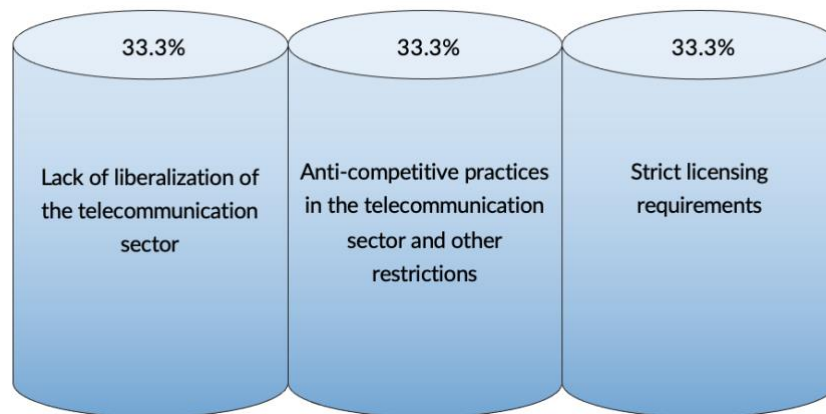
Such a licence scheme counts as ‘1.’

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.

The weights for each indicator

As shown in figure 13, each indicator is given equal weight.

Figure 13. Pillar 5's indicators and the weights



Pillar 6. Cross-border data policies

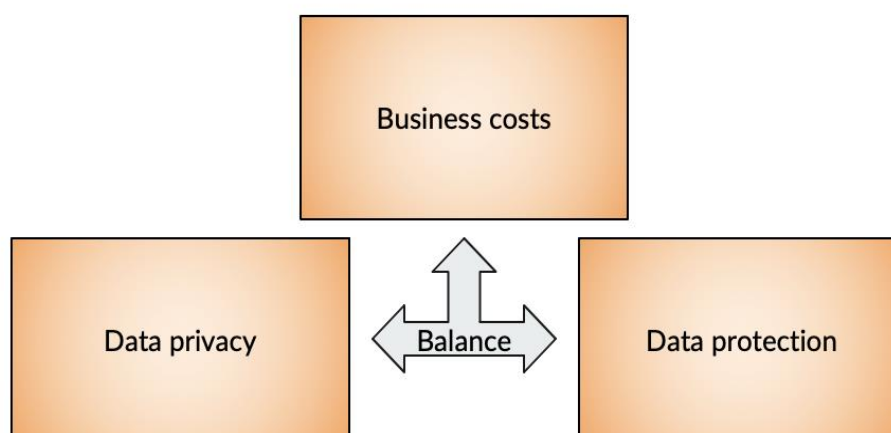
Pillar 6 deals with cross-border data policies. By regulating the ways in which data flows from one jurisdiction to another, the data policies prevent data from flowing in a laissez-faire manner. Among the different policy objectives that serve as parameters for forming a cross-border data policy, important are business costs, data privacy and data protection (figure 14).

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 gets 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 14). Compliance with data protection rules increases costs. However, the better protected that data privacy is, and the stronger 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 are, stronger accountability mechanisms would exist.

Figure 14. Balance in 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, an IP address, cookie ID, as well as health-related data and data revealing racial or ethnic origin, beliefs, and religion; (2) 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. The 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 personalise advertising and marketing.

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

- Conditions of local storage, processing or infrastructure; and
- Conditions of consent, evaluation or approval.

Conditions of local storage, processing or infrastructure

This indicator asks whether there are requirements on the location of data. The requirements could take the following forms:

- **‘Local storage requirements’** mandate 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;
- **Local processing requirements’** mandate 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). The local processing requirements are more demanding than the local storage requirements because, generally, the definition of processing includes storage. This means that a local processing requirement often presupposes a local storage requirement, while also potentially raising the cost of a foreign firm obliged to locally process the data. 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 to them;

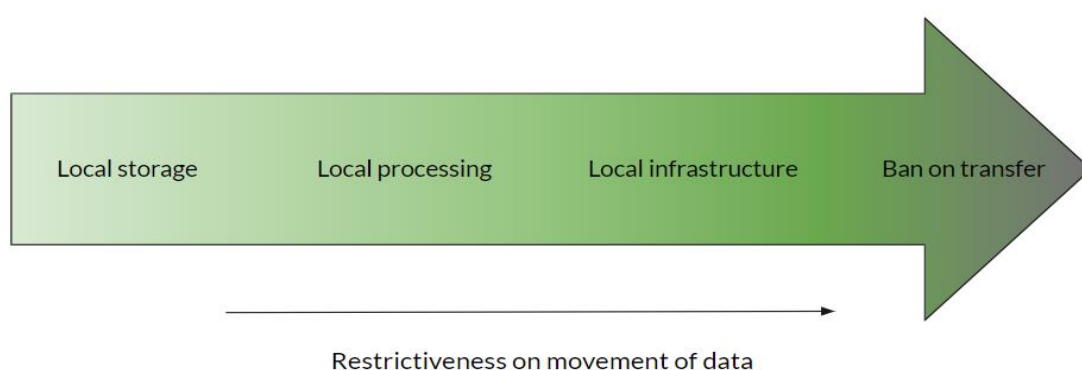
- **‘Infrastructure requirements’** mandate an establishment of a local data centre as a condition to provide certain services using data. Although under a local processing requirement, businesses feel a need to build a local server, it is not mandatory. By contrast, under an infrastructure requirement, businesses are bound to do so. In this regard, this requirement is even more demanding than local processing requirements as the establishment of data centres or local servers increases the fixed costs and barriers for companies;
- **‘Bans on data transfers’** prohibit per se cross-border transfer of data. The *per se* ban on the transfer is the most costly in that data are a crucial driver of digital trade.

The following are examples of these requirements:

- Turkey requires system operators, payment institutions and electronic money institutions to collect all relevant documents and records within the economy;
- In Kenya, data may be transferred abroad on a case-by-case basis subject to the approval of the data controller or data processor;
- Viet Nam requires foreign providers of Internet services and telecommunications to store the personal data of their users in Viet Nam;
- Australia requires companies to both store and process health records, excluding personal information within Australia;
- In Malawi, there is a local storage requirement for health-related data;
- The Republic of Korea requires financial service providers that use cloud services to locally process credit and unique identification information of their users;
- Indonesia requires foreign banks and payment networks to establish a local data centre to process electronic transactions;
- 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.

The scoring metrics of Pillar 6 have three features. First, the score depends on the storage conditions for cross-border transfer. Based on the reasons provided earlier, local storage requirements will get a lower score than local processing requirements or ban the cross-border transfer of data. The local infrastructure requirement will get the highest score (figure 15). As the business costs arising from the ban and local processing requirements are quite subtle, these requirements receive equal weight (Ferracane, 2017). Second, a condition that applies to personal data will get a higher score than a condition that applies to non-personal data. Third, a horizontal condition that applies across sectors will get a higher score than a condition 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). Please note that a measure applied to the government data should not get scored. The indicator focuses on a measure potentially affecting commercial transactions.

Figure 15. Conditions of local storage, processing and infrastructure



- The score is '0' when the data is permitted to be transferred freely without any requirement;
- The score is '0.1' when the local storage requirements apply only to specific non-personal data or a specific set of data;
- The score is '0.2' when the local storage requirements apply horizontally across sectors or personal data, or when the local processing requirement or a ban on cross-border data transfer applies to a specific set of non-personal data or a specific set of data;
- The score is '0.4' when local processing or a ban on cross-border data transfer applies horizontally across sectors or personal data, or when there is an infrastructure requirement;
- The score is '1' when there are multiple measures of any of the aforementioned requirements such that the total score is summed up to '1' or higher. Indeed, the score can be in the range of 0 to 1 based on the summed score.

Generally, these requirements are found in comprehensive data laws or sectoral laws governing the health sector, financial sector (e.g., credit card information), telecommunications sector (e.g., computer traffic data), for example. Useful secondary sources include the [DTE database](#), the [OECD STRI database](#), and specialized databases by law firms such as [Linklaters](#), [DataGuidance](#), [Lexology](#) and [DLA Piper](#). The secondary sources should only serve to guide researchers to the primary sources.

Conditions of consent, evaluation or approval

This indicator asks whether an economy puts 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:

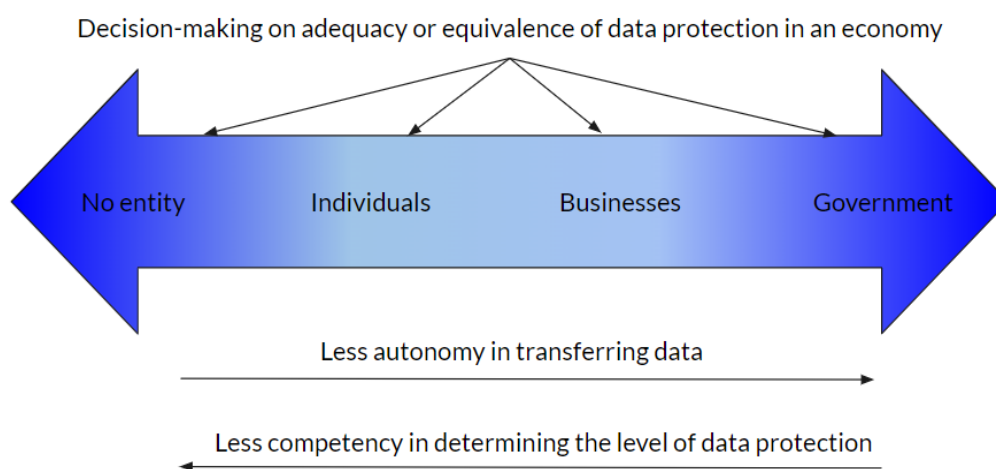
- There is no condition attached to cross-border data transfer. Thus naturally, no entity decides the question of the adequacy and equivalence of data protection in economies where data gets

transferred. In this case, economies often allow data flows across borders freely, 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, which 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 another 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 to transfer 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.

- Turkey to transfer 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 to transfer 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 types of data. 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.). As stated above, personal data carry greater value than non-personal data, and the broader the scope of applicability of a condition, the more costs it incurs. The score is ‘0’ when there is no condition. Moreover, the Government data is not listed because the database captures the commercial activities.

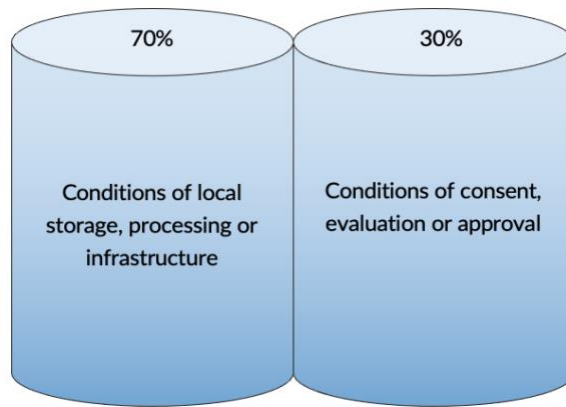
The measures are often found in a data protection law or sectoral laws with provisions governing health data, accounting data, financial data (e.g., credit card information), telecommunications (e.g., computer traffic data) etc. Useful secondary sources include the [DTE database](#), the [OECD STRI database](#), and specialized databases by law firms such as [Linklaters](#), [Data Guidance](#), [ICLG](#), [Lexology](#) and [DLA Piper](#).

The weights of the indicators

The two indicators are not equally weighted – 70% and 30% of weights are given to the indicators, respectively, as shown in figure 17. The first indicator – conditions of local storage requirements – is regarded as more weight than the other indicator because the conditions to store, process or build an infrastructure for data within the economy tend to create a higher cost of compliance. In addition, the measures may not necessarily promote digital trust. This is because the local storage does not address how data subjects’ data is to be actually used abroad.

The second indicator that deals with another set of conditions for cross-border data have less weight than the first indicator. This is because, while it incurs costs against businesses, it has rational relation 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.

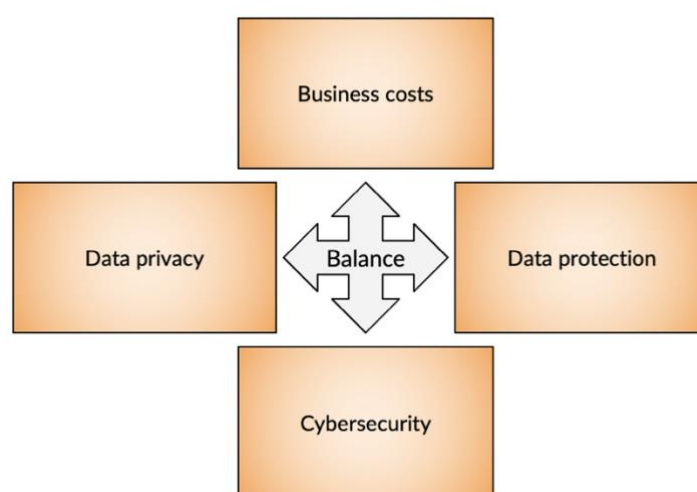
Figure 17. Pillar 6's indicators and the weights



Pillar 7. Domestic data policies

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 pillar also focuses on cybersecurity (figure 18). Cybersecurity refers to government 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 significantly impacts 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 a comprehensive data protection legal framework;
- Data retention requirement;
- Requirement to conduct a Data Protection Impact Assessment (DPIA) or appoint a Data Protection Officer (DPO);
- Government access to personal data.

Useful secondary sources include the [UNCTAD Cyberlaw Tracker](#) and specialized databases by law firms such as [Linklaters](#), [DataGuidance](#), [ICLG](#), [Lexology](#) and [DLA Piper](#). The secondary sources should only serve to guide researchers to the primary sources.

Lack of a comprehensive data protection legal framework

This indicator asks whether an economy has adopted a comprehensive data protection legal framework that applies to personal data across sectors.

As much as the need for businesses to benefit from the free flow of data transfers unbridled by unnecessary regulatory burdens and compliance costs, the needs for data privacy and protection are important because they contribute to digital trust. In this regard, the lack of data protection laws can

stagnate digital trade as users become hesitant to entrust their data with businesses willing to transfer them to other economies, and businesses and organizations can be liable for the consequences of data breaches.

Compounding this problem is the fragmentation of data protection in different sectors. Sectoral data protection obligations such as in finance, health, education and so on, can be under interoperability (PECC and Access Partnership, 2021). Often, several sectors are intertwined 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 are, in some jurisdictions, categorized also as a financial entity. Thus, different data privacy and data protection requirements require businesses to navigate through the complexities of regulations and thereby increase compliance burdens.

Accordingly, the scoring metrics for this indicator consider not only whether an economy has data protection laws, but also whether the data protection law remains fragmented, sector by sector. 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.

Data retention requirement

This indicator asks whether an economy imposes 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 at its premises upon request by the authorities.¹⁰

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 of time, 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

¹⁰ 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.

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 either set out a minimum period of retention or a maximum period of retention:

For 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.¹¹ For example:

- In Malawi, there is a required data retention period of at least 7 years;
- Australia requires a telecommunication service provider to keep specific telecommunications data related to the services it offers for 2 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;
- 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 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 5 years from the date that the transaction was concluded and after the termination of the business relationship.

For the '**maximum period of retention,**' firms cannot retain data longer than necessary. Often, requirements with a maximum period apply terms such as "as long as necessary" "as needed for legal claims" or "legitimate business purposes," instead of specifying a period. Although businesses have latitude under this type of requirement in determining whether to retain data, limitations on the period during which businesses can draw value from personal data are considered as costly. For example:

- The Republic of Korea requires data controllers to destroy personal information upon the fulfilment of the purpose of processing the information.

The score is '1' when the minimum period of data retention requirement and/or more than one maximum period of data retention requirement is applied. The score is '0.5' when the maximum period

¹¹ 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.

of data retention is in place. The score is ‘0’ when there is no requirement. Moreover, the government data is not listed because the database captures the commercial activities.

Requirement to appoint a DPO or to perform a DPIA

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.¹² 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;
- Turkey 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 Turkey, a contact person for the data controller must be appointed. However, if a data controller is located outside Turkey, a national representative, either a natural or juristic person, must be appointed;
- The Ghana 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 separate officer with expertise in compliance with data laws across economies. Compounding this is that, unlike the European Union’s General Data Protection Regulation (GDPR), data protection laws in developing economies often fragment. It is difficult for a data protection officer, even if appointed, to navigate through divergent data protection laws. A less cost alternative could be to make the appointment voluntary as an option to show companies’ data privacy policies and practices.

The score is ‘1’ if there is more than one sectoral measure or if the measures apply horizontally to all sectors. The score is ‘0.5’ if the requirement applies only to a specific sector. The score is ‘0’ when there is no requirement.

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 create exploitable vulnerabilities in other accounts as well, 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;

¹² 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).

- Allowance by Japan for a public prosecutor or a judicial police officer to request, without a warrant, a telecommunications carrier for interception and other necessary cooperation to implement interception.

If this requirement applies, the score is ‘1’, unless the score is ‘0.’

For this indicator, [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.

The weights of each indicator

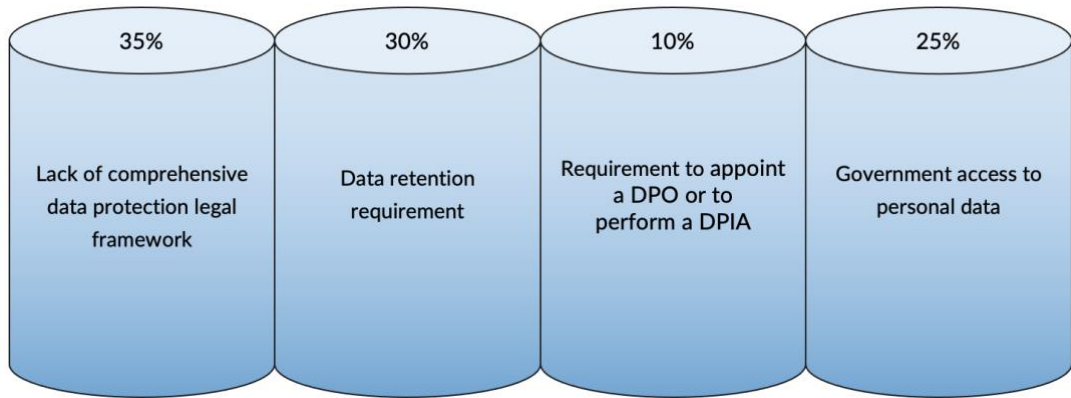
As shown in figure 19, the weights for each indicator are 35%, 30%, 10% and 25%. A lack of comprehensive data protection legal framework that applies across all sectors is given the greatest weight because having such a legal mechanism is crucial to promoting digital trust. It ensures users’ data privacy 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 data retention requirements is given the second greatest weight because, although it increases compliance cost and undermines data privacy, it is just one cybersecurity mechanism, whereas a comprehensive data protection law contains a bundle of users’ rights and data protection mechanisms and thus its impact is more prevalent.

The requirement to conduct DPIA or appoint a DPO is given the least weight. This is because such a requirement negatively affects only one policy parameter – the cost of compliance; 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.

Government access to personal data is given a weight greater than the DPO or DPIA requirement because access to such data for law enforcement purposes undercuts digital trust in the eyes of individual users. However, Government access to personal data does not have as great an impact on digital trade as the data retention requirements because, while it undermines digital trust as the data retention schemes do, government access itself does not incur *ex ante* obligation on the part of businesses and create additional burdens.

Figure 19. Pillar 7's indicators and the weights

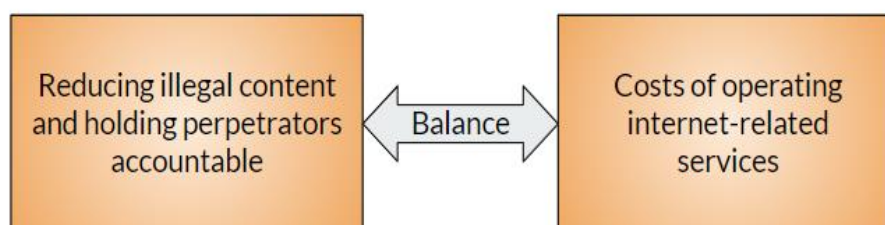


Pillar 8. Internet intermediary liability and content access

Pillar 8 deals with measures governing intermediary liability and requirements on content access. ‘Internet intermediaries’ can be defined as “the intermediaries that bring together or facilitate transactions between the third parties on the Internet.¹³ 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).¹⁴

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 in mind, the Pillar 8 consists of the following indicators:

- Safe harbour for intermediaries;
- User identity or monitoring requirements;
- Blocking or filtering of web content; and
- Licensing schemes and local/commercial presence requirements.

Safe harbour for intermediaries

This indicator asks whether an economy has a safe-harbour provision for Internet intermediaries. A safe-harbour provision protects the Internet intermediaries from legal liability for certain activities performed by their users. The scope of the safe-harbour provisions varies, as follows:

- Some jurisdictions protect the intermediaries from legal liability for copyright-infringing materials in their platforms, and illegal activities were forbidden by other laws unless the intermediaries contributed to them or had notice of them beforehand;

¹³ There is no agreed definition of intermediaries. For more information, see the Oxford Handbook of Online Intermediary Liability (Frosio, 2020); *see also* (OECD, 2011).

¹⁴ 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.

- Other jurisdictions protect the intermediaries from legal liability only for copyright-infringing activities but not for illegal activities;
- Still, other jurisdictions do not have a safe-harbour provision for them, meaning that the intermediaries are, *per se*, legally responsible for their users' activities.

Regulating content in violation of copyrights or otherwise illegally by holding Internet intermediaries hosting such content liable even when the intermediaries do not notice of it 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 score is '1' for lack of a safe-harbour provision for the intermediaries. The score is '0.5' for a safe-harbour provision that protects them from liability only for copyright-infringing activities but not from other illegal activities. The score is also '0.5' when the scope of the safe harbour remains unclear, i.e., the extent to which the intermediaries are not liable. The score is '0' for a safe-harbour provision that protects the intermediaries from legal liability for copyright-infringing materials and other illegal activities on their platforms.

Useful secondary sources 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.

User identity or monitoring requirements

The entry asks whether an economy imposes user identity requirements and other monitoring requirements.

The '**user identity requirement**' mandates that internet intermediaries require their users to supply accurate personal information to use their services or networks. For example:

- In Rwanda, electronic communications service providers must ensure that their users supply accurate personal information when using a service or a network according to the Law Governing Information Communication and Technologies.

The '**monitoring requirement**' obliges the intermediaries to monitor the users' activities and remove or block content that is deemed illegal to avoid legal liability due to such content. 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;
- The Regulation of Interception of Communications Act of Uganda 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.

These measures can be costly in that they are obliged to act as “gatekeepers” of the internet, policing their users and content on behalf of the Government. This requires substantial efforts for the intermediaries to ensure that their users supply accurate personal information and monitor anything that is posted, shared or transferred by the users through the platform.

The score is ‘1’ if at least one of such measures is implemented.

The secondary sources for this indicator include the [DTE database](#), the reports by the [Global Network Initiative](#), the [World Intermediary Liability Map](#) and the [NTE](#) report. The secondary sources should only serve to guide researchers to the primary sources.

Blocking or filtering of 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;
- Turkey 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).¹⁵ 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.

¹⁵ For the clarification of each blocking technique, see <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/>.

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.

Licensing schemes and local/commercial presence requirements

This indicator asks whether an economy imposes any licensing scheme or local or commercial presence requirements 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 only covers ISPs, excluding telecommunication facilities and service providers, which are already covered by Pillar 5, as well as e-commerce platforms, which are covered by Pillar 11.

The **‘local presence requirement’** requires companies to have a representative office or a local agent within the economy to do business. Under the **‘commercial presence requirement,’** companies must establish their own offices, branches or subsidiaries within the economy to do business. In this regard, the commercial presence requirement tends to create more costs than the local presence requirement. Hence, the score is ‘1’ for a comprehensive licensing scheme or a commercial presence requirement or when there is more than one measure for a sector-specific licensing scheme. The score is ‘0.5’ for a sector-specific licensing scheme¹⁶ or a local presence requirement.

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.

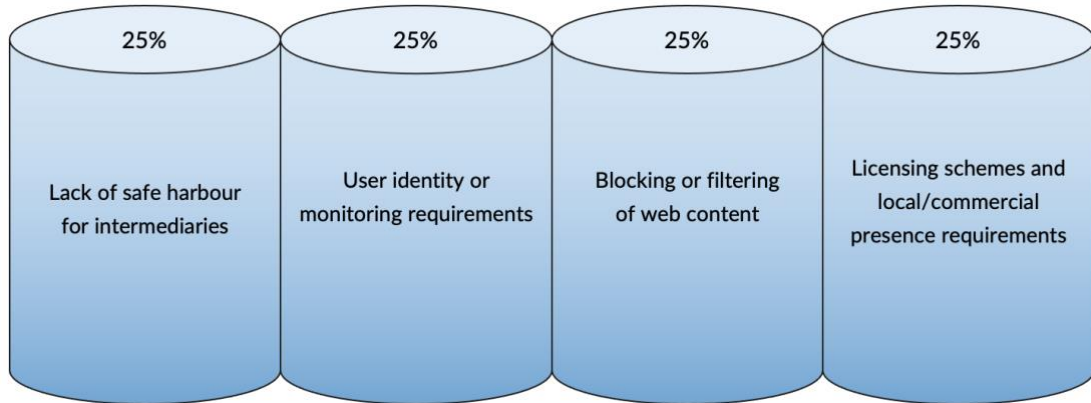
The weights for the indicators

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 indicator, without the safe-harbour provision in place or with an unclear or limited scope, the intermediaries face a higher risk of being liable for their users’ activities and the costs of litigation. The second indicator on user identity and monitoring requirements imposes upon the intermediaries additional responsibilities and thus incurs costs. The intermediaries have to 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 the third indicator. Blocking or filtering, whether performed by a government or intermediaries, directly interrupt

¹⁶ For example, Thailand requires an operator of the digital television program to obtain a license.

the intermediaries in performing their services as well as having an impact on their users. The last indicator of licensing schemes is burdensome and costly for Internet intermediaries that, by nature, have to operate across borders to hire a local representative or establish infrastructure abroad.

Figure 21. Pillar 8's indicators and the weights

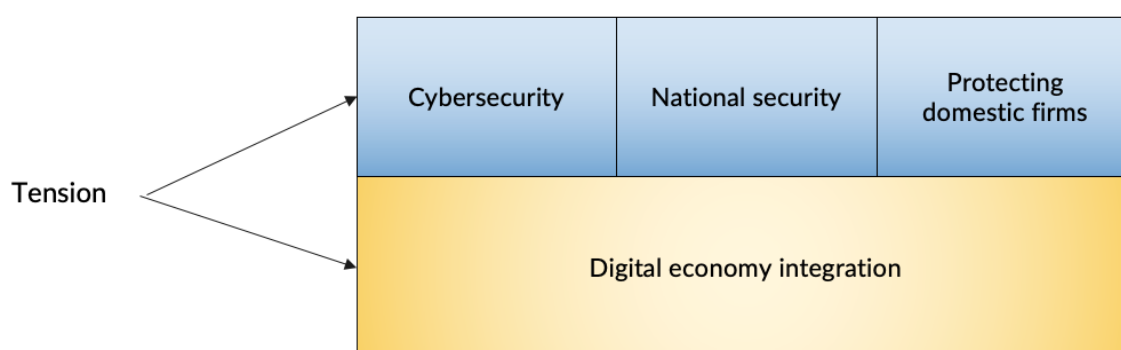


Pillar 9. Non-technical NTMs

Pillar 9 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 ICT 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 22.

Figure 22. Tension among different policy objectives in Pillar 9



Pillar 9 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 for the commercial market; 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 [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 of 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 to import transmission apparatus for radio broadcasting or television, television cameras, digital cameras and video camera recorders. In Botswana, 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.

The score is ‘1’ for trade-blocking measures such as quotas. The score is ‘0.5’ for each restriction that adds regulatory compliance costs to trade in ICT goods such as licences, permits, authorization, registration, labelling requirements and import controls.¹⁷ Otherwise, the score is ‘0.’

Researchers should look at official laws, regulations, notifications, and other measures. The secondary sources are [WTO I-TIP](#), the [Global Trade Alert](#) databases, the [NTE](#) reports, as well as reports by international organizations. The secondary sources should only serve to guide researchers to the primary sources.

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.

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).¹⁸ 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 [NTE](#) report, as well as complaints from companies and trade associations should only serve to guide researchers to the primary sources.

¹⁷ 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.

¹⁸ Harmonised System (HS) is an international nomenclature provided by the World Customs Organization for the classification of products. The HS Code adopted a six-digit code system to classify goods (WCO, 2016).

Export restrictions on ICT goods and online services

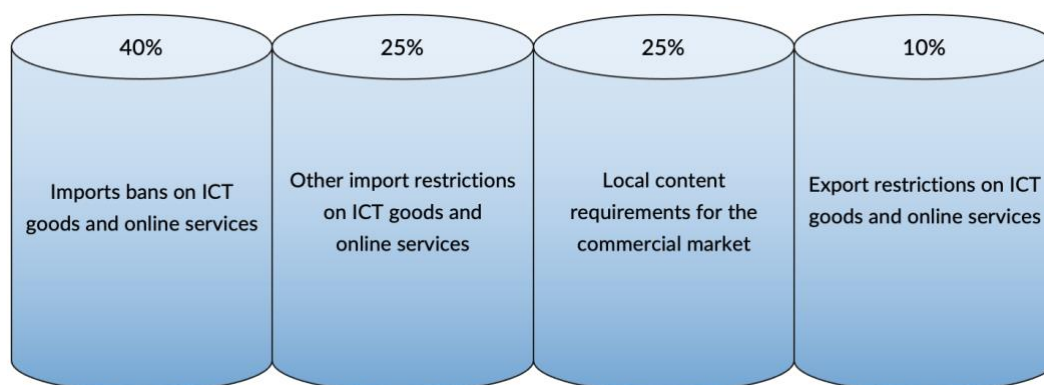
This indicator covers export restrictions on ICT goods and services. These restrictions include export bans, export licences and other restrictions limiting the number of goods to be exported or services. The score is ‘1’ if at least one of such measures is implemented.

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 [NTE](#) report, as well as complaints from companies and trade associations should only serve to guide researchers to the primary sources.

The weights for the indicators

As shown in figure 23, the weights of each of the indicators are 40%, 25%, 25% and 10%. The first indicator on import bans gets the highest weight of 40% as it completely prohibits imports. Indicators on other import restrictions and local content requirements equally receive a lesser weight of 25% because these measures limit the flows of ICT goods and online services as well as discriminate against foreign businesses. In particular, 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 aforementioned 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.

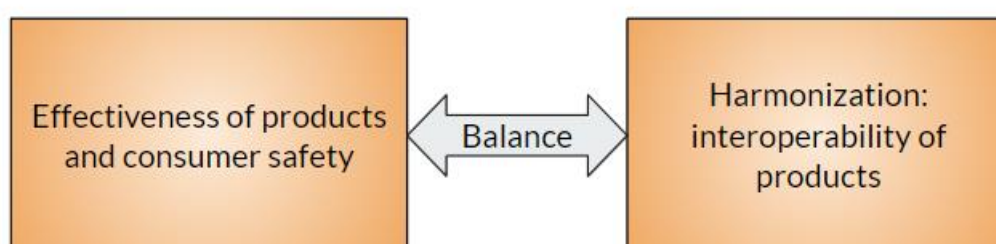
Figure 23. Pillar 9’s indicators and the weights



Pillar 10. Technical standards and related procedures

Pillar 10 covers technical standards and related procedures that can function as a trade restriction on ICT goods and online services in the telecommunication sector in a digital economy. 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 increase the interoperability of products and services across the region (figure 24).

Figure 24. Balance in different policy objectives in Pillar 10



Pillar 10 measures the interoperability of regulation in the following indicators:

- Transparency of technical standards regime;
- Self-certification for product safety (radio transmissions, EMC/EMI);
- Product screening and testing requirements; and
- Requirements on encryption standards and trade secrets.

Transparency of technical standards regime

This indicator asks whether foreign participation is not allowed in standard-setting in sectors relevant to digital trade, including the telecommunication sector, ICT goods and online services, and whether the standard-setting is not transparent. For example, Australia provides 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 for product safety (radio transmissions, EMC/EMI)

This indicator asks whether an economy allows self-certification of product safety by suppliers. In general, exports of electrical products must comply with domestic standards of radio transmissions, electromagnetic interference (EMI) or electromagnetic compatibility (EMC).¹⁹

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 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.

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.²⁰ For example:

- New Zealand requires companies that use a 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;

¹⁹ 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).

²⁰ 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.

- 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 lab outside of 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 with 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 TVs and 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](#), 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.

Requirements on encryption standards and trade secrets

The indicator covers requirements on encryption standards and trade secrets. 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).²¹ 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

²¹ Encryption is a principal application of cryptography. Cryptography refers to the technological means to secure information and communications systems (OECD, 2015).

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 4); and (b) whether an economy has requirements to disclose trade secrets or sensitive proprietary information in the process of certifying products that contain encryption. 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).²²

The score is '1' if at least one of such measure is implemented.

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 be only serve to guide researchers to the primary sources.

²² 3GPP (3rd Generation Partnership Protection) develops mobile broadband standards, such as GSM, LTE and 5G specifications (3GPP, 2008).

Box 4. 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- and 128-bits block ciphers (ISO/IEC 18033-3: 2005). Significantly, these international encryption standards serve as a baseline for the encryption algorithms.

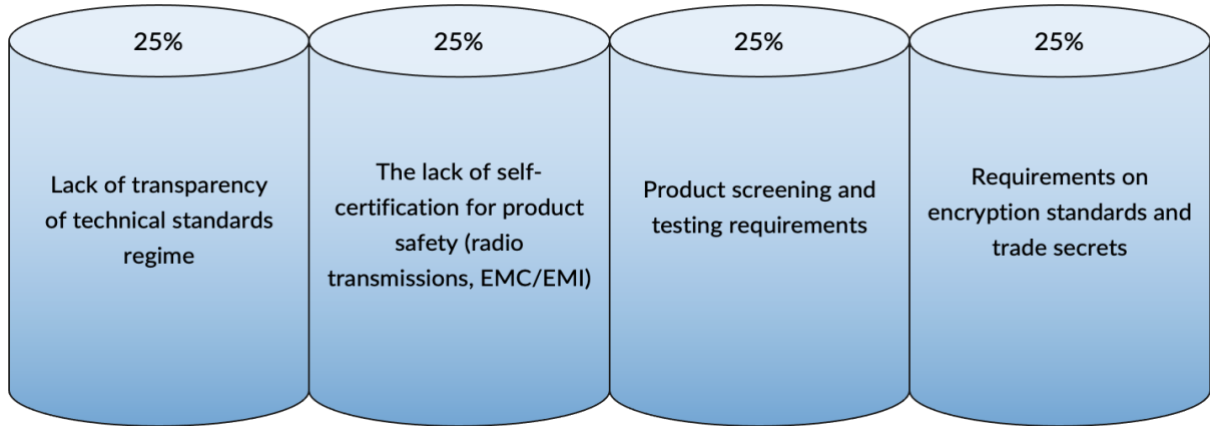
The encryption algorithms can be classified into ‘symmetric key based’ and ‘asymmetric key based’. First, symmetric encryption algorithms refer to when there is one private key for both encryption and decryption. The commonly used algorithms under this type are, for example, the Advanced Encryption Standard (AES) which 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) which 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 the indicators

As shown in figure 25, an equal weight of 25% is given because each indicator discourages foreign businesses from operating their businesses in certain economies. 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 fourth indicators, regarding non-transparent and encryption standards that differ from internationally recognized standards, lead to a lack of interoperability. 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. The fourth indicator, in relation to the mandatory disclosure of trade secrets, impacts business competition. In addition, the second and third Pillars provide additional layers to the importation of ICT goods or services, resulting in increasing business costs and slowing down the process. These measures have the potential to be implemented specifically to discriminate against foreign businesses.

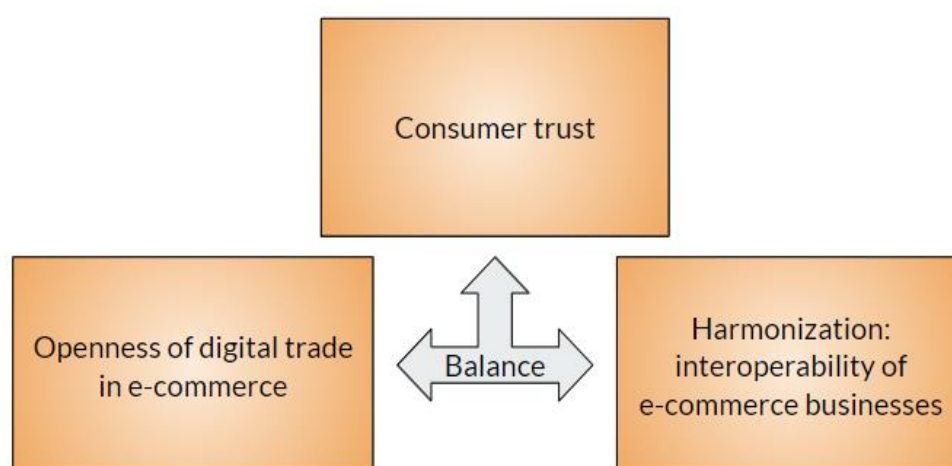
Figure 25. Pillar 10's indicators and the weights



Pillar 11. Online sales and transactions

Pillar 11 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 online sales, delivery, advertising, online payment and domain names 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 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 26.

Figure 26. Balance in different policy objectives in Pillar 11



Based on this understanding, Pillar 11 reflects the following issues:

- Requirements on online sales, delivery, and advertising;
- Requirements on online payments;
- Low threshold for *de minimis* rule;
- Requirements on domain name; and
- Lack of legal framework for online purchases.

Requirements to online purchases, delivery of online purchases and online advertising

The indicator covers requirements on online sales, including requirements on the delivery of products bought online and online advertising. The measures could be:

- Bans, licensing requirements or other requirements for e-commerce platforms. For example, the Philippines bans foreign ownership of retail trade enterprises with paid-up capital of less than US\$ 2.5 million. India provides that B2B e-commerce must not have more than one vendor that accounts for more than 25% of sales;
- 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 USD 50 threshold;

- Limitations affecting online advertising (excluding requirements that advertising should not be misleading). For example, Pakistan prohibits the broadcasting of advertisements produced in India or featuring Indian actors and characters.

For a trade-blocking measure such as certain bans on electronic commerce, the score is ‘1.’ For a measure that does not block trade per se but discourages digital trade such as licensing requirements, specific limits on market share or the number of imports via e-commerce, and requirements on advertisements, the score is ‘0.5.’ Otherwise, the score is ‘0.’

Researchers should look at official laws, regulations, and other measures. Secondary sources, such as the [DTE database](#) and the [OECD Digital STRI](#) should serve as guidance for the primary sources.

Requirements to online payments

The indicator covers requirements on 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 deviate from international standards;
- Ceilings on the maximum amount that can be paid by electronic payment methods;
- Requirements mandating the use of specific intermediaries for online payments.

For each measure, the score is ‘1.’ Requirements for ‘cryptocurrencies’²³ 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 [DTE database](#) and the [OECD Digital STRI](#) should serve as guidance for the primary sources.

Low threshold for De Minimis rule

The indicator asks whether an economy adopts a *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. The index calculates the valuation ceiling based on Special Drawing Rights (SDR).²⁴

²³ 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).

²⁴ 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.

If no *de minimis* rule exists, a score ‘1’ is given. If an economy adopts the *de minimis* rule below 133 SDR, a score ‘0.5’ is given.²⁵ However, if the *de minimis* rule is equal to or above 133 SDR, a score ‘0’ is given.

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.

Requirements on domain name

The indicator covers requirements on commercial domain names.²⁶ 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.

A score of ‘0.5’ is given if companies are required to obtain a local domain name in order to engage in electronic commerce or if they need to have a local administrative contact to do business. If, instead, a commercial presence is required in order to use a local domain name, then a score of ‘1’ is assigned. 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.

Researchers should look at official laws, regulations, and other measures. Secondary sources such as the [DTE database](#) should serve as guidance for the primary sources.

Lack of legal framework for online purchases: electronic transactions, e-signatures, consumer protection

The indicator asks whether an economy lacks legal frameworks that are relevant to online purchases. The legal frameworks that this indicator considers are (a) domestic laws of consumer protection, (b) the UNCITRAL Model Law on Electronic Commerce (1996) (MLEC), (c) the UNCITRAL Model Law on Electronic Signatures (2001) (MLES), and (d) the United Nations Convention on the Use of Electronic Communications in International Contracts (2005) (the Electronic Communications Convention).

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 MLEC and MLES are model laws 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

²⁵ The threshold 133 SDR is based on the International Chamber of Commerce (ICC) recommendation of establishing a global baseline of *de minimis* value of at least 200 USD (UNECE, 2012).

²⁶ 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.

means, attribution of data messages, acknowledgement of receipt and determining the time and place of dispatch and receipt of data messages (UNCITRAL, 2018a).

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).

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 5).

If the economy has not signed and ratified or adopted in part any of the mentioned international frameworks, the score is '1.' If the economy did not have consumer protection laws that can apply to online purchases, the score is also '1.' Although an economy has consumer protection laws, if the economy has adopted fully or in part both Model Laws but has not ratified the Electronic Communications Convention, then the score assigned is '0.5.' If an economy adopts consumer protection laws, is ratified to the Convention, and adopted the Model Laws fully or in part, the score is '0.'

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.

Box 5. Relationship among the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures and the United Nations Convention on the Use of Electronic Communications

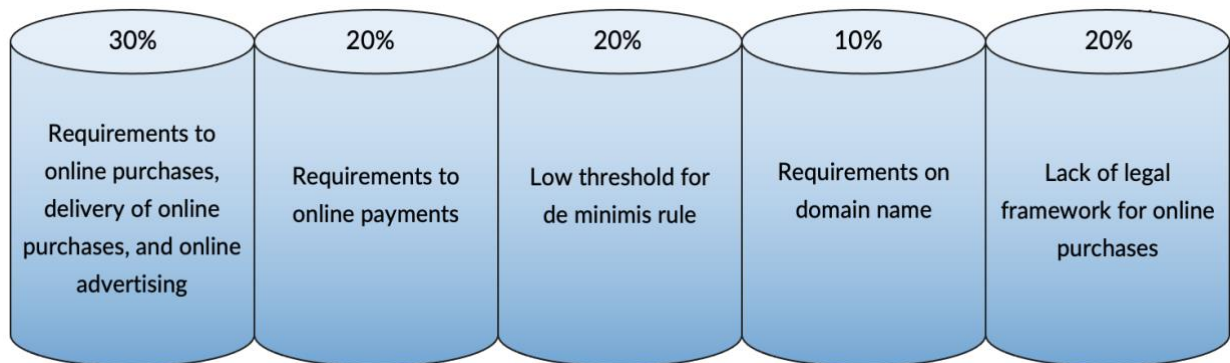
The MLEC is the first model legislative text that adopts the principles of non-discrimination, technological neutrality and functional equivalence. The principle of non-discrimination provides that a document must not be denied legal validity or enforceability solely on the grounds that it is in electronic 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. Currently, 15 States are parties to the Convention.

The weights for the indicators

As shown in figure 27, the weights for each indicator are 30%, 20%, 20%, 10% and 20%. The first indicator is given the greatest weight because requirements on sales *per se* or requirements on delivery or advertising set up direct barriers for vendors to engage in digital trade or reach consumers. The second indicator – requirements on online payments – is given a lesser weight as the requirements do not necessarily block sales or promotion of goods but make cross-border payments in electronic commerce cumbersome. The third indicator is also given 20% because the lack of *de minimis* rule does not block flows of goods but tends to increase the prices of imports. The last indicator is also given the same weight since the lack of consumer protection law that applies to electronic commerce undermines trust in the eyes of consumers, and the lack of legal recognition of electronic signatures and transactions creates uncertainty in the eyes of vendors. The fourth indicator is given the least weight because requirements on domain names for vendors do not have as much impact as the other requirements.

Figure 27. Pillar 11's indicators and the weights



Chapter 4 Concluding remarks



Initiated by ESCAP, in collaboration with ECA and ECLAC, RDTII 1.0 is a step towards addressing challenges in creating high-quality and internationally comparable indicators for the analysis of the digital-trade policy environment.

The RDTII 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 with its 11 pillars provides a roadmap to 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 meet their needs and priorities.

This document should be considered a living document to be updated as United Nations Regional Commissions and other partners continue to work together to improve the index and the data collection process. The United Nations ESCAP, ECA, and ECLAC expect 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 guideline to evaluate and achieve evidence-based policy design and adjustments will be provided upon request, in collaboration with interested international and other organizations.

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

Tariff and Trade Analysis

Tariff and Trade Analysis option within the Advanced Query provides you with multiple tariff types and sophisticated queries by including multiple reporters, partners, products, and years in a single query. You can also define aggregates. Advanced Queries can be saved and reused. This is particularly useful for more complex deviations, international and domestic tariff peaks, minimum and maximum rates, etc. [More details...](#)

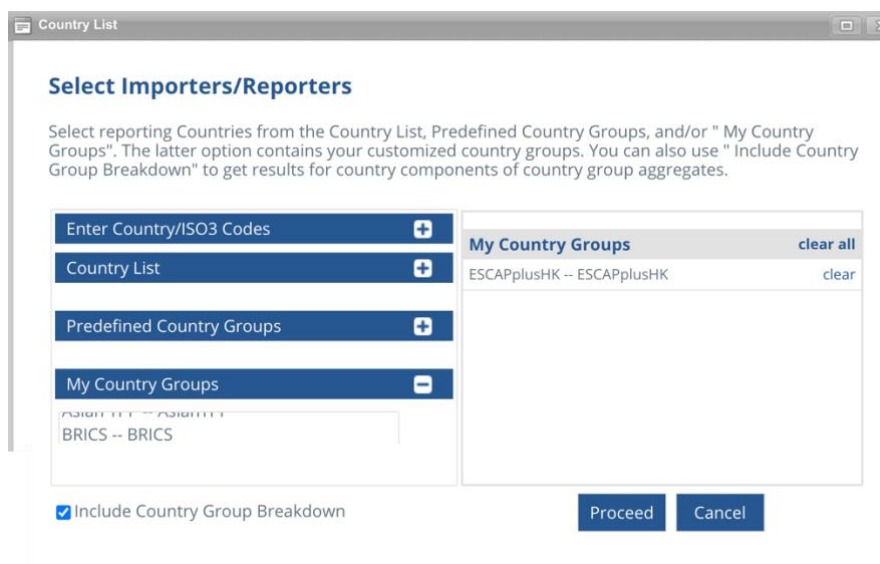
New Query Existing Query - Select a Query -

Query Name:

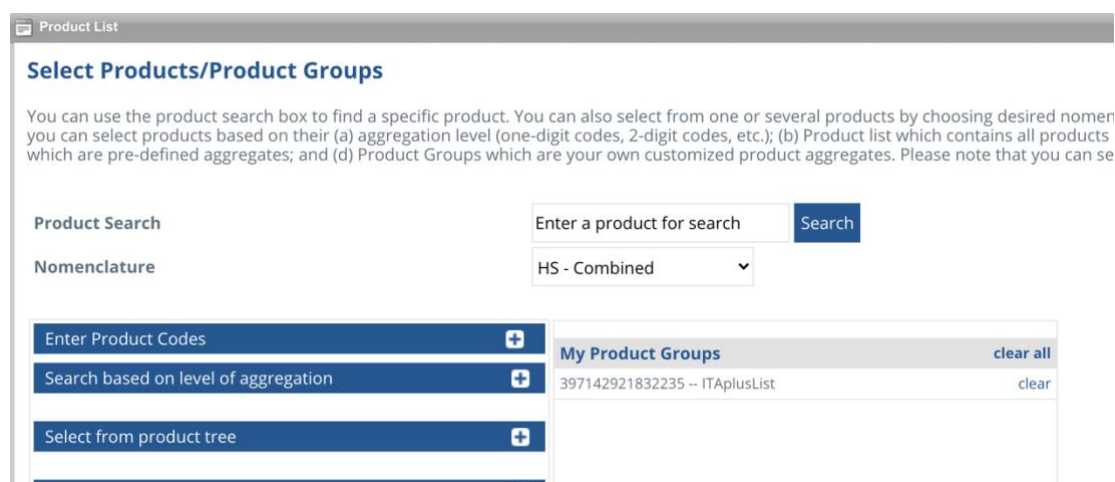
Query Description:

Data Source:

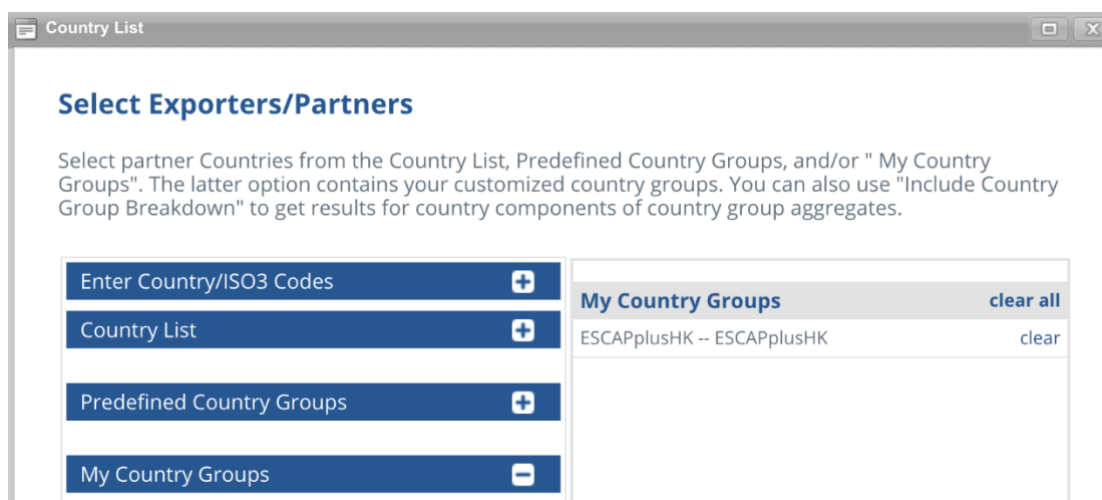
3. As Importers, select the economy of interest or select all ESCAP economy as economy group and select ‘Include economy group breakdown.’



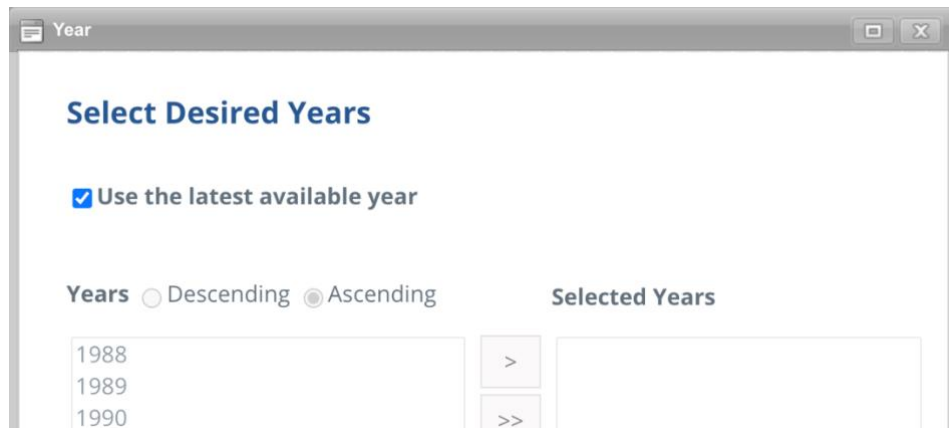
4. Select 'HS - Combined' nomenclature and select products.



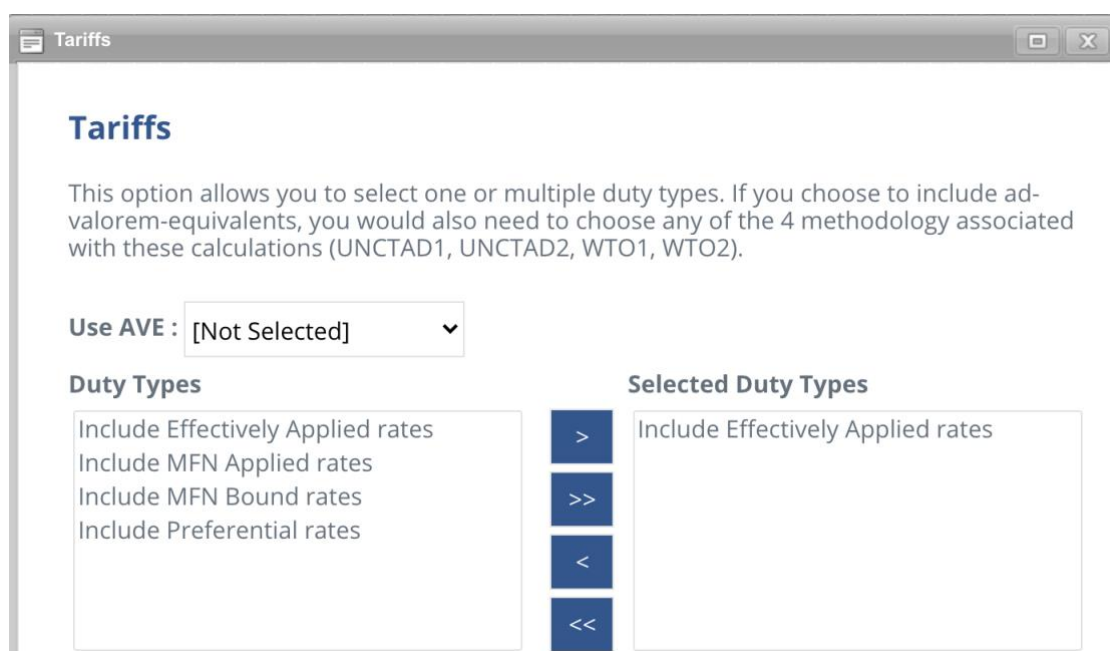
5. For Exporters, select economies.



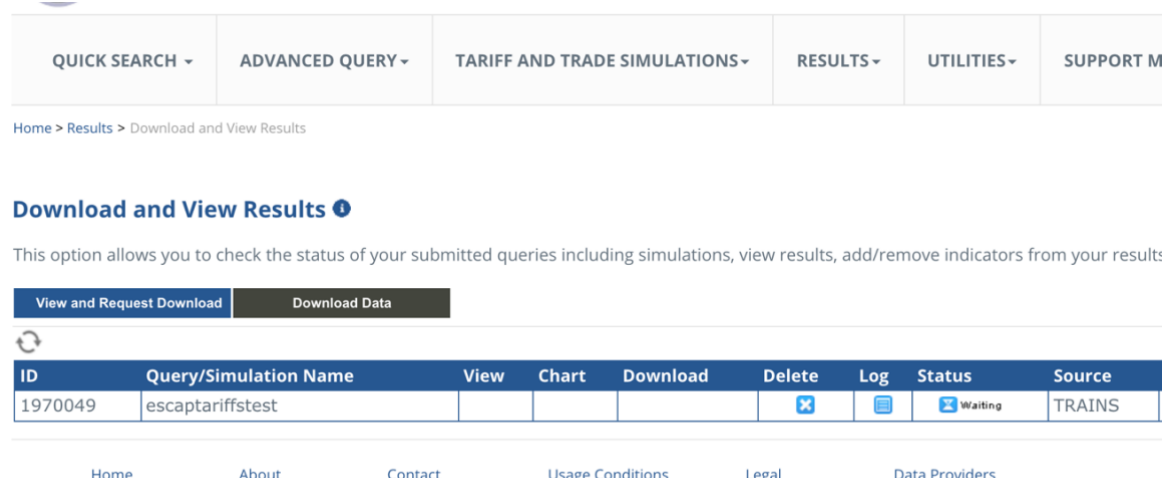
6. As Year, select the latest year available.



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.’



ID	Query/Simulation Name	View	Chart	Download	Delete	Log	Status	Source
1970049	escaptariffstest						In Progress	TRAINS

9. Click 'Download.'

ID	Query/Simulation Name	View	Chart	Download	Delete	Log	Status	Source
1970049	escaptariffstest						Completed	TRAINS

10. Select 'excel.'

WITS - Download Report

Job Name:

Job Description:

File Format: Excel

Please note that Excel can save the first 1,048,576 rows and remaining will be truncated.

11. Select also 'Nbr of Free Lines' (Number of Free Lines) and then click 'Download.'

Select Report Columns

Available Columns

- Count_Of_SAvgRates_Cases
- Sum_Of_Squared_Rates
- Minimum Rate
- Maximum Rate
- Nbr of AVE Lines
- Nbr of NA Lines
- Nbr of Free Lines**
- Nbr of Dutiable Lines
- Nbr of Total Lines
- Nbr of DomesticPeaks
- Nbr of InternationalPeaks

Selected Columns

- Partner Name
- Tariff Year
- Trade Year
- Trade Source
- DutyType
- Simple Average
- Weighted Average
- Standard Deviation
- Minimum Rate
- Maximum Rate
- Nbr of Total Lines





Pivot Header : Partner Name | Pivot Data : Nbr of Free Lines

Select |
 Select |
 Cancel | Download | Save Template & Proceed

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.'

Download and View Results

Once you choose the download option from "Download and View Results screen", you can

View and Request Download	Download Data				
					
ID	Query/Simulation Name	Save	Delete	Status	Source
2182948	escaptariffstest			 Completed	TRAINS

Annex II. ITA I and ITA II products

The list of products covered under the WTO ITA I and ITA II according to the Declaration on The Expansion of Trade in Information Technology Products.²⁷ Attachment A provides the lists of the HS 2007 subheadings. The partially covered subheadings are identified with the symbol “ex”. Attachment B provides the lists of specific products to be covered by the Declaration, whether they are classified in the HS 2007.

Attachment A

Item	HS 2007	ex	Product Description
001	350691	ex	Optically clear free-film adhesives and optically clear curable liquid adhesives of a kind 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
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

²⁷ Available at

<https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN15/25.pdf&Open=True>.

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
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 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 fibers 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
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 stands therefor
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

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
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
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 to 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
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
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

Attachment B

Item	Product Description
192	<p>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 to 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.</p> <p>For the purpose of this definition the following expressions mean:</p> <ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> "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 the 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 the 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 the 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	<p>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)</p>
194	<p>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)</p>
195	<p>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 in engineered shapes for insertion into apparatus of HS subheadings 844331, 844332 or 844339</p>

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

²⁸ The tariff elimination for printed matter shall only affect the rights and obligations with respect to trade in goods, that is, it shall not affect market access other than tariffs of the participants. Nothing in the ITA expansion agreement shall prevent an ITA member from regulating the content of such goods, including Internet content, among other things. Nothing in the ITA expansion agreement shall affect a member's market access rights and obligations on trade in services or prevent a member from regulating its services market.

References

- ABLI (2020). Transferring Personal Data in Asia: A Path to Legal Certainty and Regional Convergence. Singapore: Asian Business Law Institute. Available at <https://www.abli.asia/NEWS-EVENTS/Whats-New/ID/134>
- Anant, V., Donchak, L., Kaplan, J., and Soller, H. (2020). The Consumer-Data Opportunity and the Privacy Imperative. McKinsey and Company, 27 April. Available at <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>
- 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/>
- CBPRs (2019). APEC Cross-border Privacy Rules System, Policies, Rules and Guidelines. Cross-Border Privacy Rules System, November. Available at <http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf>
- 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>
- European Commission (2018a). What Constitutes Data Processing? Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en#answer
- _____ (2018b). What is a Data Protection Impact Assessment (DPIA) Required? Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en
- FCC (2016). Equipment Authorization APEC TEL MRA. Federal Communications Commission. Available at <https://www.fcc.gov/general/equipment-authorization-apec-mra>
- Ferracane, M. F. (2017). Restrictions on Cross-Border Data Flows: a Taxonomy. 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. 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.
- 3GPP (2008). About 3GPP. Available at <https://www.3gpp.org/about-3gpp>

- 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>
- 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, 12 August. Available at <https://www.bcg.com/publications/2019/global-trade-goes-digital>
- Lee-Makiyama, H. (2011). Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA). ECIPE Working Paper, No. 04/2011. Brussels: ECIPE. Available at <https://www.econstor.eu/bitstream/10419/174847/1/ecipe-wp-2011-04.pdf>
- 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.
- _____ (2015). OECD Guidelines for Cryptography Policy. Available at <https://www.oecd.org/sti/ieconomy/cryptography.htm>
- _____ (2018). Trade and Cross-border Data Flows. Working Party of the Trade Committee, Trade and Agriculture Directorate, 21 December. Paris: OECD Publishing. Available at [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP\(2018\)19/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En)
- _____ (2019). The Impact of Digitalisation on Trade. Available at <https://www.oecd.org/trade/topics/digital-trade/>
- PECC and Access Partnership (2021). Pacific Economic Cooperation Council. 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>
- Rucz, M. and S. Kloosterboer (2020). Data Retention Revisited. European Digital Rights, 28 September. EDRI: Brussels, Available at https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

- 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
- UNECE (2012). Trade Facilitation Implementation Guide: De Minimis. Available at <https://tfig.unece.org/contents/de-minimis.htm>
- 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
- WCO (2016). What is the Harmonized System (HS)? Available at <http://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx>
- 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
- Zidane, O. (2021). Global E-Commerce and the Impact of COVID-19. Infomineo, 24 November. Available at <https://infomineo.com/global-e-commerce-and-the-impact-of-covid-19/>



United Nations
Economic and Social Commission for Asia and the Pacific
Trade, Investment and Innovation Division
United Nations Building, Ratchadamnoen Nok Avenue
Bangkok 10200, Thailand
Email: escap-tiid@un.org
www.unescap.org