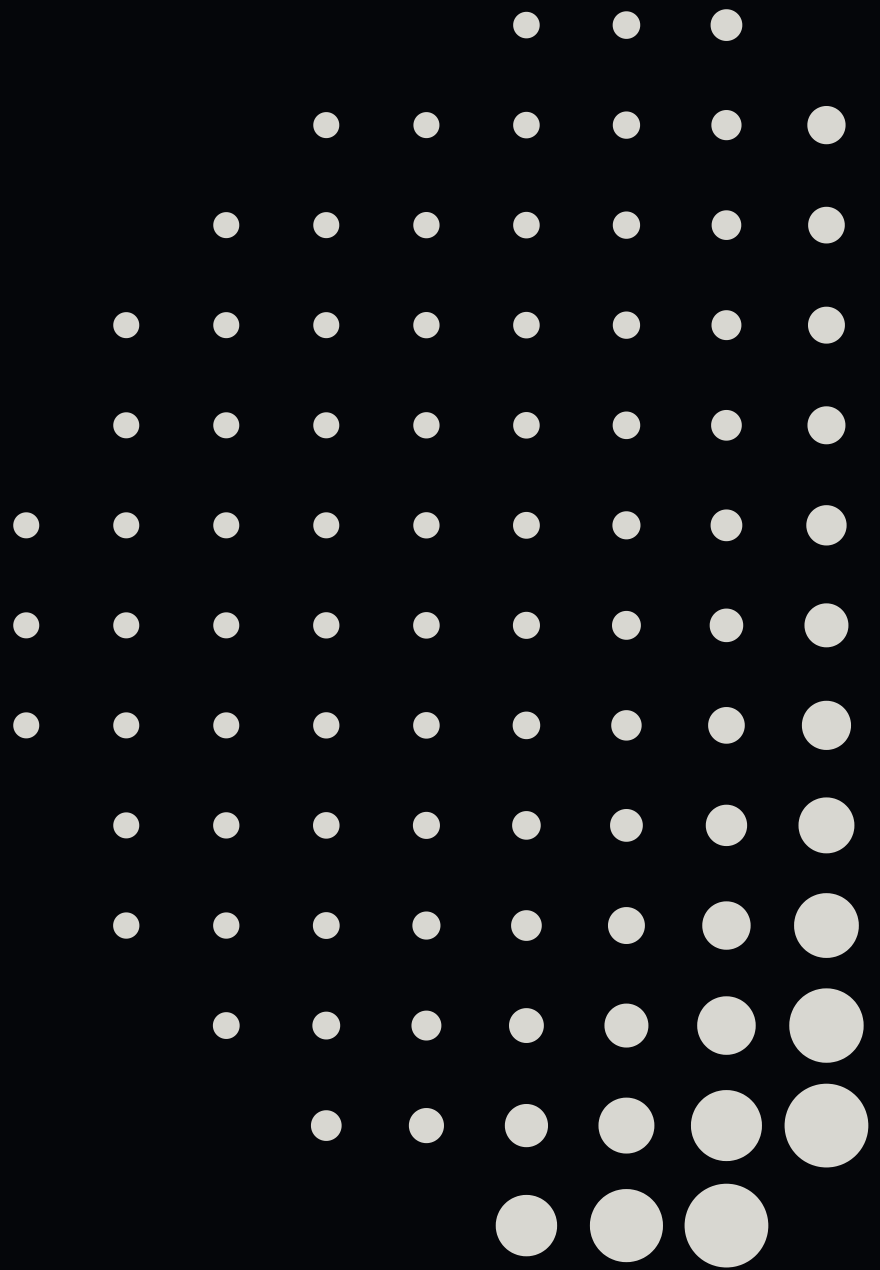




Pakistan Data Observatory



METHOD AND CODEBOOK

Transparency Safeguard Index

How ten federal data systems were read, coded and scored

AUTHOR

Nuzaina Faisal Khan

EDITION

First edition, October 2026

METHOD

Version 0.1

ONLINE

pakistandataobservatory.org/method

Contents

1	What the index measures	3
2	What the index does not measure	3
3	The legal setting	3
4	Which systems are on the register	3
5	The nineteen questions	5
6	How an answer is coded	10
7	Close calls	10
8	The score	11
9	Why the score is built this way	12
10	How far to trust a number	13
11	Agency replies	14
12	Changes	14
13	References	14

About this document. This is the full method behind the Transparency Safeguard Index: the selection rule, the nineteen questions and their coding rules, the formula, a worked example and the robustness checks. A short version is on the website. Each system's record, with its sources, is at pakistandataobservatory.org/systems.

Author. Nuzaina Faisal Khan, founder, Pakistan Data Observatory.

Suggested citation. Khan, N. F. (2026). *Transparency Safeguard Index: method and codebook*, version 0.1. Pakistan Data Observatory. pakistandataobservatory.org/method

1 What the index measures

The Transparency Safeguard Index (TSI) measures what a public body has published about one of its data systems. It has two halves. Transparency covers what the agency says about the system: its purpose, its legal basis, the data in it, who else gets that data, and which reports on it are public. Safeguards covers what the agency says about protection: the rules on use and retention, how a person can see or correct a record or complain, and what is said about breaches and outside audit.

A score is a statement about the public record on a given date. Every answer on every record links to the page it came from or lists the places that were searched.

2 What the index does not measure

It does not measure whether a safeguard works, and it does not measure whether one exists. An agency may hold an internal retention schedule or a security certificate and have said nothing about either. That agency scores zero on those questions, and the record says "not found", which is accurate.

The reverse also holds. A published policy is not proof that the policy is followed.

The index was built this way because disclosure is the part that can be checked from outside. Anyone can open the same pages and reach the same answer or show that the answer is wrong. It is also a legal duty in its own right. Section 5 of the Right of Access to Information Act, 2017 requires federal public bodies to publish their functions, the laws and rules they work under, their policies and decisions, and their finalised audit and performance reports.

3 The legal setting

Article 14(1) of the Constitution protects "the dignity of man and, subject to law, the privacy of home". Article 19A gives every citizen "the right to have access to information in all matters of public importance". Pakistan has no data protection law in force. A Personal Data Protection Bill has been through consultation and has not been passed by Parliament.

In June 2026 the Ministry of Information Technology and Telecommunication published a consultation draft of a National Data Governance Policy. It is still a draft. Fourteen of the nineteen questions here cite one of its clauses, because it is the government's own most recent statement of what public bodies should do with data. Twelve of those fourteen also rest on a principle of the OECD Privacy Guidelines or a provision of the Right of Access to Information Act. Two rest on the draft alone: T2.3, on hosting and transfers abroad, and S2.4, on finding out who has looked at a record.

The draft policy provides for an official National Data Maturity Index (clause 18.3), in which a government authority assesses public bodies. The TSI is a different exercise. It is a reading from outside, limited to what a citizen can find.

4 Which systems are on the register

A system qualifies if it meets at least two of these four conditions. Each record lists the ones it meets.

- it holds records on at least a million people or covers the whole country
- enrolment is mandatory or cannot practically be avoided
- it holds identity, biometric, health, financial, location or communications data
- its records are used to decide something about an individual

The first edition has ten systems, all run by federal bodies, so that every record is read against the same information law.

Three systems on the original list could not be assessed. On 8 October 2026 the sites of the Election Commission of Pakistan, the Pakistan Telecommunication Authority and the Sehat Sahulat Programme could not be opened from a connection outside Pakistan. An answer of "not found" is only honest if the place was actually searched, so the three were set aside and will be assessed from inside the country. A Pakistani abroad who wants to read those sites meets the same wall.

Systems that were considered and are not on the register:

System	Agency	Why it is not on the register
Sehat Sahulat Programme information system	Ministry of National Health Services, Regulations and Coordination, with NADRA as technical operator	Meets the selection rule. Not assessed: on 8 October 2026 pmhealthprogram.gov.pk returned 'Currently this service is not available in your region' to a browser outside Pakistan. To be assessed from a connection inside Pakistan and added to the register.
Device Identification, Registration and Blocking System (DIRBS)	Pakistan Telecommunication Authority (PTA)	Meets the selection rule. Not assessed: on 8 October 2026 dirbs.pta.gov.pk and pta.gov.pk timed out to a browser outside Pakistan. To be assessed from a connection inside Pakistan and added to the register.
Electoral rolls	Election Commission of Pakistan (ECP)	Meets the selection rule. Not assessed: on 8 October 2026 ecp.gov.pk returned 'Web Page Blocked!' to a browser outside Pakistan. To be assessed from a connection inside Pakistan and added to the register.
Punjab Safe Cities surveillance network	Punjab Safe Cities Authority	Provincial. The first edition covers federal bodies only, so that every record is read against the same information law. It meets the selection rule and is a candidate for a later edition, where T3.1 would be coded against the Punjab Transparency and Right to Information Act 2013.
SIM subscriber records and biometric verification	Mobile operators, under PTA regulation, verifying against NADRA	Meets the selection rule, but no single public body holds the data: mobile operators keep the subscriber records, PTA regulates, NADRA verifies. The index needs one responsible agency per record.
One Patient, One ID	Ministry of National Health Services, Regulations and Coordination; Ministry of IT and Telecommunication	Not yet fully operational. APP reported on 6 October 2026 that the two ministers 'agreed on a joint roadmap to make it operational soon'. Score it once it is live nationally.
State Bank of Pakistan EasyData	State Bank of Pakistan	A statistics portal. It holds no personal data, so it fails the selection rule.

5 The nineteen questions

Each question has four coding rules: what counts as disclosed, as partly disclosed, as not found, and when the question cannot apply. The source each question is drawn from is given beside it.

What each agency is asked

T1 System disclosure What the system is for, the law behind it, the data in it and who is responsible.	T2 Flows and sharing Who else gets the data, who builds or runs the system, and where it is stored.	T3 Accountability records How to ask for information, and which audits and assessments are public.
S1 Rules on use Whether there is a privacy notice, a retention rule and limits on other uses.	S2 Individual rights Whether a person can see their record, fix an error, complain, and find out who looked.	S3 Security and oversight What is said about breaches and independent security audits.

T1 System disclosure

T1.1 Does the agency say what this system is for and what it is used to decide?	
☒ Disclosed	The agency's own site or an official document describes the system's purpose AND at least one decision or service it supports.
☐ Partly disclosed	The system is named and described only in general terms (for example in a press release or annual report), with no statement of what it is used to decide.
☐ Not found	The system is not described in any official source, or is known only from court records, leaks or press reporting.
☐ Not applicable	Never.
Drawn from	OECD Openness; RTI s.5(1)(a); RTI s.5(1)(d)

T1.2 Does the agency cite the law, rule or notification this system runs under?	
☒ Disclosed	The agency, when describing this system, cites a specific statute, rule, regulation or notification by name and year.
☐ Partly disclosed	The agency cites only its general founding statute, with nothing specific to this system; or a law exists that plainly covers the system but the agency does not cite it anywhere it describes the system.
☐ Not found	No legal instrument is cited by the agency and none covering the system can be found.
☐ Not applicable	Never.
Drawn from	OECD Purpose Specification; RTI s.5(1)(b)

T1.3 Does the agency list the kinds of personal data this system holds?

- ☒ **Disclosed** An official source lists the categories or fields of personal data held (for example name, CNIC number, fingerprints, address, income).
- ☒ **Partly disclosed** Some fields can be read off a public form, or categories are mentioned in passing, but there is no list presented as what the system holds.
- ☐ **Not found** No description of the data held.
- ☐ **Not applicable** Never.
- Drawn from OECD Openness; NDGP cl. 9.4

T1.4 Is there a named office or officer responsible for the data in this system, with contact details?

- ☒ **Disclosed** A post or person identified, by title or by the source's own words, as responsible for this system or for the personal data in it (for example a data officer, or a director-general of the named registry), with a working contact route.
- ☒ **Partly disclosed** Only a general agency helpline, complaint cell or head-office address; or a named head of IT or software whose stated remit does not mention this system or its data.
- ☐ **Not found** No contact route that mentions the system or its data.
- ☐ **Not applicable** Never.
- Drawn from OECD Accountability; NDGP cl. 16.4

T2 Flows and sharing**T2.1 Does the agency say which other public bodies receive or can query this data?**

- ☒ **Disclosed** Recipient bodies are named in an official source in connection with access to this data, or are a class fixed by law whose members are officially listed elsewhere (for example all licensed banks), or a list or register of data-sharing arrangements is published.
- ☒ **Partly disclosed** Sharing is acknowledged ("shared with government departments", "under data sharing protocols") without naming recipients; or individual arrangements are announced in press releases but there is no list.
- ☐ **Not found** No statement on sharing.
- ☐ **Not applicable** Only if an official source states the data is shared with no one.
- Drawn from OECD Use Limitation; NDGP cl. 10.4

T2.2 Does the agency name the companies or outside bodies that build or run this system?

- ☒ **Disclosed** The outside builders or operators of the system (companies, or other public bodies acting as contractor) are named in an official source, with what each does. Where the data is hosted is a separate question (T2.3).
- ☒ **Partly disclosed** A vendor is named in a tender award or press release with no statement of its role or access to data; or contractors and their roles are acknowledged but some or all are not named.
- ☐ **Not found** No vendor information.
- ☐ **Not applicable** Only if an official source states the system is built and run entirely in-house.
- Drawn from RTI s.5(1)(e); OECD Openness

T2.3 Does the agency say where the data is stored and whether any of it leaves Pakistan?

- ☒ **Disclosed** An official source states where data is hosted (in-country or not, and by whom) AND whether any is transferred abroad.
- ☒ **Partly disclosed** One of the two is stated.
- ☐ **Not found** Neither is stated.
- ☐ **Not applicable** Never. A cloud-hosted system is exactly where this matters.
- Drawn from NDGP cl. 8.2; NDGP cl. 13.1

T3 Accountability records**T3.1 Has the agency named an official who answers information requests, and said how to file one?**

- ☒ **Disclosed** A designated official under the RTI Act is named with contact details AND the way to file a request is explained.
- ☒ **Partly disclosed** One of the two.
- ☐ **Not found** Neither.
- ☐ **Not applicable** Only if the body is outside the RTI Act (for example a provincial body, in which case code against the provincial RTI law and say so in the note).
- Drawn from RTI s.9; RTI s.5(1)(h)

T3.2 Are audit, evaluation or performance reports that cover this system published?

- ☒ **Disclosed** At least one report from the last three years that assesses this system specifically (audit, evaluation, inquiry or performance report) is published.
- ☒ **Partly disclosed** The agency's annual report or an Auditor General report mentions the system without assessing it, or the only report is more than three years old.
- ☐ **Not found** No report covering the system.
- ☐ **Not applicable** Never.
- Drawn from RTI s.5(1)(i); NDGP cl. 18.4

T3.3 Has a privacy or data protection impact assessment of this system been published?

- ☒ **Disclosed** A privacy impact assessment, data protection impact assessment or equivalent is published in full or in substantial summary.
- ☒ **Partly disclosed** An official source states that an assessment was done, but it is not published.
- ☐ **Not found** No assessment is mentioned.
- ☐ **Not applicable** Never.
- Drawn from NDGP cl. 11.4; OECD Accountability

S1 Rules on use

S1.1 Is there a privacy notice or data policy that covers this system?

- ☒ **Disclosed** A document issued as a policy, notice, protocol, charter or terms that names this system or the service it supports and says how personal data in it is used. It counts whoever it is addressed to (the people in the system, or bodies asking for the data).
- ☐ **Partly disclosed** Only a website privacy statement (cookies, web forms); or an agency-wide policy that does not mention the system; or the use of the data is explained only in help text such as an FAQ.
- ☐ **Not found** No privacy notice of any kind.
- ☐ **Not applicable** Never.

Drawn from OECD Openness; NDGP cl. 11.7

S1.2 Does the agency say how long records in this system are kept?

- ☒ **Disclosed** A retention period, or a rule for deletion or disposal, is stated for the records in this system.
- ☐ **Partly disclosed** Retention is stated for some records only, or only as "as long as necessary" or "as required by law" with no period.
- ☐ **Not found** Nothing on retention.
- ☐ **Not applicable** Never. A permanent register should say it is permanent; that statement counts as full.

Drawn from NDGP cl. 11.9; OECD Use Limitation

S1.3 Does the agency state limits on using this data for anything beyond its stated purpose?

- ☒ **Disclosed** A statute, rule or policy states that the data may be used only for listed purposes, or sets conditions for any other use.
- ☐ **Partly disclosed** A general confidentiality or secrecy provision applies (for example an offence for staff who disclose records) but nothing limits what the agency itself may use the data for.
- ☐ **Not found** No limit is stated.
- ☐ **Not applicable** Never.

Drawn from OECD Purpose Specification; OECD Use Limitation

S2 Individual rights

S2.1 Does the agency explain how a person can see their own record?

- ☒ **Disclosed** A published route, online or in person, by which a person can view or obtain the data held about them in this system, in any form (a certificate, an app screen, a printed extract). One consolidated procedure is not required.
- ☐ **Partly disclosed** A person can check a status or a single field (for example "check your registration") but not see the record.
- ☐ **Not found** No route to see one's own record.
- ☐ **Not applicable** Never.

Drawn from OECD Individual Participation; NDGP cl. 12.6; NDGP cl. 6.11

S2.2 Does the agency explain how a person can get an error in their record corrected?

☒ **Disclosed** A published correction or modification procedure, with what to submit and where.

☐ **Partly disclosed** Correction is mentioned as possible, with no procedure.

☐ **Not found** Nothing on correction.

☐ **Not applicable** Never.

Drawn from OECD Individual Participation; NDGP cl. 12.7

S2.3 Is there a complaint route for misuse of this data, with a stated response time?

☒ **Disclosed** A complaint route that covers data misuse or data errors in this system AND a stated time limit for a response.

☐ **Partly disclosed** A general complaint route with no time limit, or one that does not mention data.

☐ **Not found** No complaint route.

☐ **Not applicable** Never.

Drawn from OECD Accountability; NDGP cl. 11.7

S2.4 Can a person find out who has accessed their record?

☒ **Disclosed** A published way for a person to see who accessed or verified their record, and when.

☐ **Partly disclosed** The person is notified of, or must consent to, some accesses (for example third-party verification) but cannot see a history.

☐ **Not found** No access transparency.

☐ **Not applicable** Never.

Drawn from NDGP cl. 12.3; NDGP cl. 6.11

S3 Security and oversight**S3.1 Has the agency committed to telling people about data breaches, or published a record of past ones?**

☒ **Disclosed** A published commitment to notify affected people of a breach, or a published record of past incidents and what was done.

☐ **Partly disclosed** The agency has publicly acknowledged a specific incident (statement or press release) but has no standing commitment or record.

☐ **Not found** Neither.

☐ **Not applicable** Never.

Drawn from OECD Security Safeguards; NDGP cl. 11.8

S3.2 Does the agency say who independently audits the security or data handling of this system, and how often?	
☒ Disclosed	An official source names an independent auditor or a certification with a date (for example an external audit or a named security standard), and its frequency or validity.
☐ Partly disclosed	Security measures or "regular audits" are asserted, with no auditor, standard or date.
☐ Not found	Nothing on security or audit.
☐ Not applicable	Never.
Drawn from	OECD Security Safeguards; NDGP cl. 18.4

6 How an answer is coded

Disclosed scores 1. **Partly disclosed** scores 0.5. **Not found** scores 0. **Not applicable** is left out of the average and needs a written reason.

An answer of disclosed or partly disclosed must rest on an official public source: the agency's own website or app, a statute, rule or gazette notification, an official report, or a reply to an information request that has been published in full. The record quotes the passage and links to the page. A copy of the page is saved.

Press reports, reports by other organisations and Wikipedia are used to find things and are never the evidence for a code. If a newspaper reports that an agency holds a security certification and the agency has not said so itself, the answer is "not found".

An answer of not found comes with a list of the pages that were opened and the date. The search starts with the agency's own site and the system's own site or app listing, then the governing law and rules, then the agency's reports. The list on each record says exactly where the search went, so that anyone can repeat it or point to the page it missed.

A document sent privately does not change a code. If an agency publishes it, the code changes.

7 Close calls

Five questions and one general point needed a reading rule. Each was settled once and applied to every system.

T1.4, responsible officer. A named head of IT or software counts as partly disclosed. Full credit needs a post that the agency's own page ties to the system or its data, such as a director-general of the named registry.

T2.1, recipients. Recipients count as named when the agency names the bodies, or defines them as a class fixed by law whose members are officially listed, such as all licensed banks. A formal register of sharing agreements is not required.

T2.2, vendors. The outside builder or operator counts whether it is a company or another public body. Hosting is asked separately in T2.3.

S1.1, privacy notice. A published policy, protocol or charter that names the system and says how personal data in it is used counts in full, whether it is addressed to the people in the system or to bodies requesting the data. An FAQ counts as partly disclosed.

S2.1, seeing your record. Any published route by which a person can obtain their own record counts, including a certificate or an app. A single named procedure is not required.

Undated documents. Some rules depend on how old a document is. Where a document's date cannot be established, the agency gets the benefit of the doubt.

8 The score

$$TSI = 100 \times \sqrt{\left(\frac{1}{3} \sum_{k \in T} D_k\right) \times \left(\frac{1}{3} \sum_{k \in S} D_k\right)}$$

$$D_k = \frac{1}{n_k} \sum_{i \in k} x_i$$

D_k = mean of the applicable indicator codes in sub-dimension k
 T = mean of D_T1, D_T2, D_T3
 S = mean of D_S1, D_S2, D_S3
 TSI = 100 * sqrt(T * S)

Codes are averaged within each of the six groups. The three group scores in each half are averaged to give Transparency (T) and Safeguards (S). The TSI is one hundred times the square root of T multiplied by S. It is rounded to one decimal place for display and nowhere else.

A worked example, using a made-up system:

Example Records System (fictional)

No.	Code	Meaning
T1.1	1	Disclosed
T1.2	0.5	Partly disclosed
T1.3	0.5	Partly disclosed
T1.4	0	Not found
T2.1	0.5	Partly disclosed
T2.2	0	Not found
T2.3	0	Not found
T3.1	1	Disclosed
T3.2	0.5	Partly disclosed

No.	Code	Meaning
T3.3	0	Not found
S1.1	0.5	Partly disclosed
S1.2	0	Not found
S1.3	0	Not found
S2.1	0	Not found
S2.2	0	Not found
S2.3	0.5	Partly disclosed
S2.4	0	Not found
S3.1	0.5	Partly disclosed
S3.2	0	Not found

Group	Name	Score
T1	System disclosure	0.5

Group	Name	Score
T2	Flows and sharing	0.2
T3	Accountability records	0.5
S1	Rules on use	0.2
S2	Individual rights	0.1
S3	Security and oversight	0.3
Transparency		0.4
Safeguards		0.2
TSI		26.5

9 Why the score is built this way

Three codes and no rescaling. The scale follows the Ranking Digital Rights Corporate Accountability Index, which scores full disclosure 100, partial 50 and no disclosure found 0, with "N/A excluded from the score and averages" (2017 Index report, section 1.4). Because every question is already on the same scale, no normalisation is applied. Methods such as min-max rescaling depend on the other units being scored, so adding an eleventh system would change the scores of the first ten (Nardo et al. 2008, pp. 27 to 30).

Equal weights. There is no evidence on which to say that one group of questions matters more than another by any particular amount. Equal weighting is the usual choice in that position. The OECD and JRC Handbook notes that it "could also disguise the absence of a statistical or an empirical basis" (Nardo et al. 2008, p. 31). That is true here, and the answer is the range printed beside every score, which shows what the score would be under ten thousand other sets of weights.

Averaging by group first. The groups have between two and four questions. Averaging all nineteen together would let a group count for more only because it was split into more questions. The cost is the reverse effect: each of the two questions on security and oversight carries more weight than each of the four on individual rights. The leave-one-out table below shows how much.

A geometric mean between the two halves. With an ordinary average, a high score on one half makes up for a low score on the other: "a deficit in one dimension can thus be offset (compensated) by a surplus in another" (Nardo et al. 2008, p. 33). An agency that describes its system in full and says nothing about protection would land in the middle of the table. Under a geometric mean it does not. With T at 0.80 and S at 0.10, the ordinary average is 45.0 and the TSI is 28.3. The Human Development Index made the same change in 2010 for the same reason (UNDP 2010; Munda and Nardo 2009). Within each half an ordinary average is used, because zeros are common and a geometric mean at that level would reduce most groups to zero.

One consequence: if either half is zero, the TSI is zero. Transparency and Safeguards are always printed beside it.

10 How far to trust a number

Every score is recomputed five ways. The tables are generated from the data and change whenever a code changes.

System	TSI	Range if weights change	Ordinary average	Partial worth 0.25	Partial worth 0.75	Partial worth nothing	Question that moves it most	Change when removed
PDO-01 Civil registry and national identity database	63.9	48.0 to 76.9	63.9	55.6	72.2	47.2	T2.1	-4.4
PDO-02 IRIS taxpayer system	52.9	44.0 to 62.0	54.9	43.1	61.9	31.9	S3.2	-5.8
PDO-03 Passport issuance system	31.7	16.4 to 45.5	31.9	21.8	41.5	11.8	S2.2	-3.3
PDO-04 Integrated Border Management System (IBMS)	21.4	11.7 to 29.3	28.5	13.5	28.8	0.0	S1.1	-7.4
PDO-05 National Socio-Economic Registry (NSER)	52.7	42.6 to 63.2	54.2	43.2	61.7	32.9	S1.1	-5.6
PDO-06 Pakistan Citizen's Portal	36.7	25.0 to 48.8	36.8	28.8	44.6	20.8	S1.2	+5.5
PDO-07 Insured persons and employers registry	21.2	5.7 to 34.9	24.3	16.6	25.9	11.8	S2.1	-7.1
PDO-08 Electronic Credit Information Bureau (eCIB)	43.7	23.5 to 60.4	44.4	38.3	49.0	32.9	T2.1	-7.3
PDO-09 Digital Population and Housing Census 2023	39.6	21.0 to 56.4	41.0	34.0	45.3	28.3	S1.2	+6.6
PDO-10 Safe City Islamabad surveillance and analytics	10.5	2.5 to 18.1	15.3	6.7	14.0	0.0	S2.3	-10.5

Weights. Ten thousand random sets of weights are drawn for the groups, and the balance between the two halves is varied between 40:60 and 60:40. The range shown beside each TSI runs from the 5th to the 95th percentile of the results (the approach in Saisana, Saltelli and Tarantola 2005). Where two systems' ranges overlap, the method does not separate them.

Aggregation. The TSI under an ordinary average of the two halves.

Partial credit. The TSI if "partly disclosed" were worth 0.25, 0.75, or nothing.

Leave one out. Each question is removed in turn. The table gives the one whose removal moves the score most.

A single coding call can move a score by several points. In the worked example, changing one answer from not found to partly disclosed lifts the TSI from 26.5 to 32.0. For that reason the register is not ranked.

Factor analysis, principal components and Cronbach's alpha are not reported. Ten systems are too few for any of them to mean anything.

11 Agency replies

Each agency is sent its record with every answer of not found or partly disclosed listed, and asked one question: is this published somewhere that was missed? Scores are published without waiting for the reply. After 15 working days with no answer the record is marked "No reply received". A reply that points to a public source changes the code whenever it arrives.

Replies are logged on the Agency replies page. A reply is published in full only with the agency's agreement.

12 Changes

The register is re-checked in full every April and October. Corrections between those dates are made as they come in and listed here.

No changes since the first edition.

13 References

Munda, G. and Nardo, M. (2009). Noncompensatory/nonlinear composite indicators for ranking countries: a defensible setting. *Applied Economics*, 41(12), 1513–1523.

Nardo, M., Saisana, M., Saltelli, A., Tarantola, S., Hoffmann, A. and Giovannini, E. (2008). *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD Publishing.

OECD (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.

Ranking Digital Rights (2017). *2017 Corporate Accountability Index*.

Saisana, M., Saltelli, A. and Tarantola, S. (2005). Uncertainty and sensitivity analysis techniques as tools for the quality assessment of composite indicators. *Journal of the Royal Statistical Society: Series A*, 168(2), 307–323.

UNDP (2010). *Human Development Report 2010*, technical notes.

Government of Pakistan. Right of Access to Information Act, 2017 (Act No. XXXIV of 2017).

Ministry of Information Technology and Telecommunication (2026). *National Data Governance Policy*, consultation draft, June 2026.