KSC.JUSNREM INTELLIGENCE SERIES

SOVEREIGN INTELLIGENCE

Public capability, answerable to the people



POLICY PAPER PAKISTAN

KSC.JUSNREM

Evolutionary, Strategic and Anticipatory Legal Intelligence

ISSUE I · 2026

KSC-JUSNREM.IO · JUSNREM.DIGITAL

Sovereign Intelligence for Pakistan

Constitutional capability, knowledge and accountable public action

KSC.JUSNREM | Collaborative research | Issue-I 2026

Independent policy research. November 2026. This paper proposes a framework for public institutions in Pakistan. It carries no official endorsement and reports no adopted government programme or deployed system.

Four pillars of public capability

Constitutional authority and public accountability

Controllable digital infrastructure

Federated intelligence and inclusive capability

Legal memory and institutional learning

Contents

Preface: collaboration and sources of doctrine 8
Abstract 8
Executive synthesis 8
How the framework fits together 9
Reading and authority conventions 10
Part I Pillar I Constitutional authority and public accountability 11
The proposed framework and the public knowledge proposition 11
International and comparative foundations 15
Pakistan constitutional institutions and the competent actor 21
Public judgment reasons and accountable reliance 28
Institutional form and the decision dossier 36
Part II Pillar II Controllable digital infrastructure 40
Worked design one Public information cloud exit 42
Part III Pillar III Federated intelligence and inclusive capability 51
Worked design two Federated allocation of information access capacity 53
Part IV Pillar IV Legal memory and institutional learning 62
Worked design three Legal source continuity 70
Part V Institutional applications and Sovereign OS 77
Proposed implementation contracts for the four institutional applications 83
Sovereign OS as a distinct enabling architecture 85
Part VI Implementation investment and accountability 96
A capability programme before a platform programme 96

Contents continued

Responsible offices and separated decisions 98
Gates including shadow comparison 99
Baseline and evaluation contract 100
Staffing and whole life investment 102
Procurement and retained capability 103
Public safeguards and practical correction 103
Incidents continuity and reopening 105
Effect based change control 105
Expansion and orderly retirement 105
Draft procurement clauses 106
Testing the objections 106

Annex I Illustrative demonstrator planning calculation and evaluation specimens 109

Annex II Operating toolkit and gate concordance 114

Completed synthetic charter 114
Practical role separation 114
Evidence package manifest 115
Completed coordination authority record 115
Gate scheme concordance 116

Annex III Source and authority registers 117

Framework source notes 117
Legal and comparative research notes 118

Subject index 132

List of figures

Figure 1. Four pillars of public capability 39

Figure 2. Cloud exit and the human decision boundary 49

Figure 3. Illustrative cloud options over three years 50

Figure 4. Federated evidence without automatic consensus 60

Figure 5. Synthetic allocation consequences 61

Figure 6. Legal source continuity and qualified answers 76

Figure 7. The Sovereign OS three-layer interface concept 94

Figure 8. Six services and explicit trust boundaries 95

Figure 9. Evidence gates from scope to retirement 108

Figure 10. Illustrative demonstrator resources 111

List of tables

Table 1. How the framework fits together 9

Table 2. Distinguishing neighbouring fields 14

Table 3. The public-accountability chain 27

Table 4. Opaque systems: concerns and responses 33

Table 5. Four institutional options 36

Table 6. Six capacities of retained institutional control 42

Table 7. Cloud-exit evidence package 43

Table 8. Cloud options and whole-life cost 45

Table 9. Cloud dependency evidence and tests 46

Table 10. Cloud-exit test catalogue 47

Table 11. Federated allocation: planning inputs 55

Table 12. Federated allocation: options and tradeoffs 56

Table 13. Federated allocation test catalogue 58

Table 14. Knowledge infrastructure: connected functions 63

Table 15. Synthetic legal-source record 74

Table 16. Legal-source continuity test catalogue 74

Table 17. Four institutional applications 84

List of tables continued

Table 18. Sovereign OS: ideas and implementation discipline 86

Table 19. Sovereign OS interface contracts 88

Table 20. Service responsibilities and exclusions 89

Table 21. Core data objects and validation 90

Table 22. Workflow transitions and failure responses 92

Table 23. Responsible offices and separated decisions 98

Table 24. Evidence-dependent gates 100

Table 25. Evaluation: comparators and material failures 101

Table 26. Illustrative sixteen-week demonstrator sequence 109

Table 27. Illustrative staffing model 109

Table 28. Measures and interpretation limits 112

Table 29. Synthetic incident record 113

Table 30. Synthetic charter 114

Table 31. Practical role separation 114

Table 32. Coordination authority record 115

Table 33. Historical gate-scheme concordance 116

Edition record. Issue-I 2026, published November 2026; sources examined to 8 November 2026. Source-specific qualifications and access dates appear in the reference notes.

Citation form. Sovereign Intelligence for Pakistan: Constitutional capability, knowledge and accountable public action, KSC.JUSNREM, Issue-I 2026 (November 2026).

Preface: collaboration and sources of doctrine

This is a collaborative KSC.JUSNREM research contribution led by Khurram Chughtai. It applies doctrine stated in JUS.automica (KSC.JUSNREM 2026), chiefly the Sovereign Control Requirement and the Accountability Gap of chapter 18, and develops the author's Sovereign OS concept. Those works are its doctrinal sources; legal and technical sources are cited in the notes. The author's interest is declared at 6.69A.

Abstract

A public institution may remain answerable for a decision while losing the ability to examine its evidence, correct an error or continue a service without its supplier. This paper calls the sustained capacity to address that gap Sovereign Intelligence: the ability of constitutionally competent institutions to obtain, assess and use knowledge for lawful public purposes, and to govern the expertise, records and computational systems on which they depend. Its four pillars connect constitutional authority and accountability, controllable infrastructure, federated and inclusive capability, and legal memory.

Three worked synthetic designs examine cloud exit, intergovernmental allocation and legal-source continuity. Their constructed inputs and calculations show how institutions could test a proposed capability; they do not establish performance in practice. Legislative scrutiny, provincial services, fiscal and procurement oversight, and judicial research provide four settings for applying the methods. Sovereign OS supplies a separate proposed architecture for organising source-based analysis through five institutional perspectives. The implementation question is whether a responsible institution can demonstrate sufficient authority, evidence, staffing, independent evaluation and correction capacity to justify a defined use. Conventional records, research and software remain comparators throughout.

Executive synthesis

Pakistan's constitutional institutions need to remain able to establish what they know, identify what they do not know, act through the correct authority and correct consequential errors. A dependable archive, a statistical series with usable definitions, a competent research service and a professional able to recognise a missing legal premise can contribute more to that capacity than an elaborate system built on uncertain records. Artificial intelligence (AI) is one possible form of assistance, not the definition of intelligence or the source of sovereignty.

The policy problem is the separation of formal responsibility from effective ability. A department may answer for a decision while being unable to inspect the method supporting it, correct a source, obtain supplier records or continue the service after a contract ends. Conversely, technical control does not entitle the department to perform another institution's function. Sovereign Intelligence therefore joins knowledge capability with lawful competence and public accountability. It asks both whether institutions can govern their dependencies and whether affected people and competent reviewers can hold those institutions to account.

The four pillars give the proposal a stable structure. Pillar I establishes the public purpose, competent actor, evidential basis, reasons and review. Pillar II makes understanding, audit, security, modification, suspension and replacement observable capacities rather than contractual adjectives. Pillar III enables evidence exchange

and cooperation without erasing federal, provincial, local or institutional competence, and treats language and non-digital access as practical conditions of service. Pillar IV preserves sources, versions, legal relationships, actual reasons and correction history across changes in law, personnel and suppliers. No aggregate score can offset missing authority, an unlawful disclosure or an unusable correction route.

The comparative research broadens this framework without displacing it. International law distinguishes sovereign equality and cooperation from the domestic powers of particular officials. Comparative public-law decisions illustrate evidence, privacy, procedural protection and the actual influence of automated scores within their own jurisdictions. Pakistani constitutional and statutory analysis supplies the domestic enquiry. Federal Rules of Business, public finance and procurement requirements cannot be assumed to govern provincial action. Draft policies, guidelines awaiting applicable adoption and unresolved legal references retain those limitations.

The applications operate at two levels. The three worked designs contain reproducible fictional inputs, calculations, schemas and failure tests. They establish a method for examining capability, not measured national performance. The four institutional applications supply the public functions and legal consequences into which such methods might fit. Their relationship is complementary: a court's research service can use source-continuity discipline, while its adjudicative authority and procedural obligations remain distinct. A procurement review can use cloud-exit evidence, but successful restoration is not authority to award, pay, renew or terminate a contract.

The proposed first programme should establish the baseline, demonstrate bounded capability, test it independently and decide whether lawful operational reliance is justified. A maintained catalogue, transparent spreadsheet, trained research team or revised supplier contract remains a valid outcome. Shadow evaluation should not alter actual cases. Expansion requires evidence of public value, sustained expertise, usable challenge, acceptable cost and a tested fallback. The sixteen-week and PKR 10.2 million resource model is a planning illustration. It is not the selected budget, a market quotation or an approved timetable.

How the framework fits together

Element	Purpose	Must not be confused with
Four pillars	Organise constitutional and operational public capability	Four software products or four interchangeable institutions
Three analytical modes	Evolutionary, Strategic and Anticipatory Legal Intelligence examine change, options and plausible disruptions	A mechanical past/present/future division
Sovereign OS three-layer concept	Doctrinal kernel, five-lens mesh and synthesis starting from citizen reality	A grant of sovereign or institutional authority
Five lenses	Legislative, executive, regulatory, judicial and enforcement perspectives	Five constitutional branches or five equal sovereign organs
Three worked designs	Test evidence, calculation, controls and failure response	Government deployments or empirical performance results
Four institutional applications	Examine the public functions in which assistance might be justified	Replacements for the three worked designs
Implementation gates	Separate research, testing, shadow comparison and authorised reliance	Permission to publish independent scholarship

Reading and authority conventions

Part I develops constitutional authority and public judgment, including the proposed framework and the comparative and Pakistani research. Part II examines controllable infrastructure and the complete cloud-exit design. Part III develops federation, inclusion and the complete allocation design. Part IV joins the national knowledge infrastructure to the complete source-continuity design. Part V connects the four institutional applications with Sovereign OS. Part VI supplies the proposed implementation, investment and accountability programme. The illustrative resource model and the source registers follow.

The source register contains ten A-series notes and 112 B-series notes. Each identifies the source, the proposition or provisions relied on and any material qualification. Official texts, reproduced judgments, scholarship and technical recommendations are distinguished. Some source authentication, subsequent-treatment and provincial-law questions remain unresolved; the relevant notes identify those limits. Citation of an instrument does not establish its current applicability to every proposed use.

The source distinction is substantive. Primary law must be assessed for jurisdiction, scope, version and applicability. Comparative law retains its home jurisdiction. Scholarship supplies arguments and proposed doctrines. Technical recommendations supply methods, not Pakistani powers. Every number in the three worked designs and resource model is constructed. The implementation arrangements are proposals; no institution is represented as having agreed to participate.

Abbreviations

Each short form is used after the instrument or body has first been cited in full.

AI	Artificial intelligence
Constitution	Constitution of the Islamic Republic of Pakistan 1973
DNPA 2025	Digital Nation Pakistan Act 2025 (Act I of 2025)
GDPR	Regulation (EU) 2016/679, General Data Protection Regulation
MoITT	Ministry of Information Technology and Telecommunication
NIST	National Institute of Standards and Technology (United States)
OECD	Organisation for Economic Co-operation and Development
PFM Act 2019	Public Finance Management Act 2019
PKR	Pakistani rupees
PPR 2026	Public Procurement Rules 2026, SRO 1658(I)/2026
RTI Act 2017	Right of Access to Information Act 2017 (Act XXXIV of 2017)
SRO	Statutory Regulatory Order

Part I Pillar I Constitutional authority and public accountability

1.1 The expanded knowledge and public-law account strengthens the original four-pillar framework. The proposed doctrine explains the capability sought; the applicable law identifies who may exercise power and on what conditions. These are connected but different sources of authority.

The proposed framework and the public knowledge proposition

The people and the constitutional institutions

1.2 The phrase public sovereignty must be used with constitutional precision. Pakistan's Preamble locates ultimate sovereignty in Almighty Allah and describes the authority exercised by the people within the prescribed limits as a sacred trust. It provides that the State exercises its powers and authority through the people's chosen representatives. The present proposal takes the citizen-facing and representative dimension seriously without substituting an inaccurate paraphrase for that constitutional formulation. Neither software ownership nor executive access to a national dashboard is the constitutional source of public power.[A4]

1.3 Article 50 identifies Parliament as the President together with the National Assembly and the Senate. The President is therefore not outside Parliament's constitutional composition, although the Presidency and the two Houses perform differentiated functions. Article 90 places federal executive authority, subject to the Constitution, with the Federal Government consisting of the Prime Minister and Federal Ministers, acting through the Prime Minister in the President's name. Article 91 establishes the Cabinet relationship and collective responsibility to both Houses. An interface serving the Prime Minister’s Office and the Presidency must preserve these distinct constitutional functions.[A4]

1.4 This matters directly to system design. A briefing commissioned for the Prime Minister is not thereby an instruction from Parliament. An information request from an executive office is not automatically compulsory for every institution. A parliamentary oversight record is not an executive permission to amend a service. A reference to the President does not authorise software to perform a constitutional act in the President's name. Each workflow requires an institution, function, legal route and responsible office, not merely a prestigious account label.

1.5 The proposed interface therefore separates an institutional view from an authority to act. A parliamentary view may examine expenditure, dependencies, programme limitations and the reasons for policy choices within the applicable parliamentary process. An executive view may coordinate implementation and obtain advice within the relevant competence. An institution-specific records view supplies verified material for those functions. The data displayed can overlap, but the permissions, audience and legal effect do not become identical. Provinces and other institutions do not become subordinate nodes simply because the same software presents their evidence.

The research foundation and its legal status

1.6 The framework proposes a Sovereign Control Requirement: formal authority must be supported by operational capacity sufficient to remain answerable for public power. Six capacities organise the inquiry: understanding, audit, security, modification, suspension and replacement. The objective is governable dependence, not technological autarky. These are analytical proposals, not an enacted Pakistani statutory regime. The following designs translate them into evidence records and tests.

1.7 Digital standardisation can centralise authority in practice. Continuity of service is not necessarily continuity of lawful institutional command. This volume therefore proposes federation, separate authority records and a tested minimum service rather than one unrestricted national control room. Shared infrastructure is not shared legal competence. Public responsibility may involve several participants without leaving a gap in which no institution can obtain the record or correct the relevant failure.

1.8 Representative fiscal authority requires separate attention to analysis, procurement and actual spending commitments. A favourable cost comparison does not itself supply appropriation, procurement authority or authorisation to pay. An approved programme budget does not settle every contract or information-release decision. Fiscal legality constrains what the programme may commit; sovereign capability concerns whether the institution can govern the resulting dependence.

Control proportionate to public consequence

1.9 The Sovereign Control Requirement is not a demand that every routine tool be owned or internally rebuilt. The proposed framework raises the required degree of control with the seriousness, coercive effect, irreversibility and population scale of the public function. A public information page, an eligibility determination and a coercive enforcement workflow require different demonstrations of competence and control. The assessment begins with the function and its consequences, not with an undifferentiated label such as artificial intelligence.

1.10 For each service, the institution should state the consequence of failure, the availability of human correction, the duration of tolerable interruption and the dependencies it cannot presently replace. It should then explain what evidence is proportionate for the six capacities. A readily substituted public-text search service may require export and restoration evidence; a service shaping deprivation of a statutory entitlement also requires a decision record, effective challenge and a verified way to prevent an uncorrected error from continuing to operate. These are design applications of the proposed doctrine, not assertions that the same testing duties are already prescribed by every applicable law.

The Sovereign Accountability Gap

1.11 A distinct institutional failure arises where sovereignty is invoked to resist scrutiny rather than preserve public responsibility. The gap can face inward, when an institution invokes its authority to shield consequential operations from those affected, or outward, when jurisdictional claims frustrate accountability across borders. It is not cured simply by moving a system into domestic infrastructure. A locally controlled system can still deny a person reasons or a practical route to correction.

1.12 The programme should therefore apply a double test. Can the institution govern its suppliers and systems? Can the public and legally competent reviewers hold the institution to account? A proposal that answers only the first question may increase state capacity while worsening the second. Security requirements should be specified for particular records and audiences, with reviewable reasons for restrictions, rather than used as a blanket exemption from institutional explanation.

Inclusion and fiscal continuity as constitutional capability

1.13 This paper proposes a non-digital pathway where essential services or legal rights would otherwise be defeated by foreseeable exclusion. Assisted digital access and a genuinely usable alternative are not always equivalent. If authentication itself is wrong, an assistant using the same blocked interface cannot resolve the exclusion. Sovereign capability therefore includes a competent office able to accept relevant material, determine the appropriate route and correct the underlying record.

1.14 The fiscal inquiry follows the public-money circuit from authority to raise revenue through stewardship, expenditure and audit. This complements the capability inquiry: an architecture that can be purchased but cannot be staffed, maintained or reviewed within a lawful resource arrangement is not a sustainable public capability. Recurring costs, correction capacity and supplier exit should appear in the programme's fiscal account, rather than be hidden behind its initial acquisition price.

1.15 A state exercises public power through judgments about the world. It identifies needs, interprets legal obligations, distributes resources, evaluates risks and determines when intervention is justified. Each activity depends on knowledge. A decision can fail because the institution misunderstands its authority, because its evidence is incomplete, because its analysis is unreliable, or because those responsible cannot carry the decision into effect. It can also fail after implementation, when the records needed to understand an error have disappeared or the institution lacks the means to correct it. Sovereign Intelligence names the continuing public capacity needed to address these connected problems.

1.16 The definition proposed in this paper joins the capacity to know with the responsibility to act lawfully. It recognises that expertise, records, infrastructure and organisational memory help determine what a state can accomplish. It also recognises that public knowledge acquires practical significance through constitutionally constituted institutions. Evidence must reach the body empowered to consider it. A finding must be distinguishable from an assumption. A recommendation must remain open to examination. The person or institution exercising a power must answer for its consequences.

1.17 This formulation is the paper's conceptual synthesis. Its legal foundations come from identifiable bodies of law governing sovereignty, constitutional competence, public administration, rights and remedies. Its institutional implications draw on international frameworks for data and artificial intelligence. Their different legal characters matter. A treaty obligation, a constitutional judgment, an administrative directive and a voluntary technical framework contribute in different ways to the argument. The task is to explain their relationship and the institutional requirements that follow from it.

1.18 The term intelligence is used here for the production and disciplined application of knowledge. It includes research, statistics, professional expertise, institutional memory, public participation, evaluation and computational analysis. AI can assist several of these functions. The quality of the wider capability depends on the relationships among them. A system that generates fluent answers while concealing its sources may increase the volume of information available to an institution while weakening its ability to distinguish a reliable finding from a persuasive mistake. A carefully maintained record, examined by competent people and connected to a working process of review, may contribute more to a particular public function than a technically elaborate system.

1.19 Sovereign AI concerns the development, access, control and governance of AI capability within this wider account. National-security intelligence has a further specialised meaning derived from its governing laws and institutional purposes. The United States, for example, defines foreign intelligence, counterintelligence and national intelligence within its national-security legislation. The breadth adopted in this paper therefore requires attention to the particular legal regime whenever a capability is used for security collection, analysis or operations.[B1]

1.20 The definition also distinguishes legal sovereignty from effective capacity. A state may possess international legal personality and retain formal authority while depending on an external provider for essential records, analytical methods or service continuity. An institution may own its equipment while lacking the expertise to evaluate its outputs. Conversely, international cooperation may strengthen domestic capability where the institution retains lawful authority, adequate access, competent oversight and workable alternatives. The relevant inquiry concerns the consequences of a dependency for the public function being performed.

1.21 Effective control is consequently specific to a function. It includes the ability to identify the evidence on which a decision rests, understand the limits of an analytical method, supervise the use of a system and intervene when its performance becomes unacceptable. It also includes continuity. A public body needs to preserve its records, maintain access to specialist knowledge and recover its operations after a supplier, funding arrangement or technical component changes. A contractual right to export data has practical value only when the records can be exported in usable form and another competent operator can continue the work.

1.22 The word sustained gives this definition its temporal dimension. Knowledge can be lost through staff turnover, discontinued projects, obsolete formats, fragmented responsibilities and changes in institutional structure. An administration that repeatedly purchases capability without retaining the means to understand or maintain it accumulates obligations alongside assets. Sovereign Intelligence therefore encompasses succession, maintenance, preservation and learning. Its object is an enduring public ability to make and carry out justified choices.

1.23 These requirements apply across the institutions of the state. Parliament needs evidence with which to examine legislation and expenditure. Courts need dependable records and arguments that can be challenged. Executive bodies need operational knowledge and lawful means of delivery. Audit and oversight institutions need access sufficient to investigate what occurred. Universities, professions, civil society and affected communities contribute knowledge that an administration may otherwise overlook. In the framework proposed here, Constitutional, Legislative, Governance and Fiscal Intelligence describe overlapping capacities within this wider undertaking. Their connections should preserve each institution's mandate and independence.

Distinguishing neighbouring fields

Field	Main question	Relationship to Sovereign Intelligence
Sovereign AI	Who controls the models, compute, data and supply chain?	Supplies important capabilities but does not itself establish public authority or remedy
Governance Intelligence	How can administration improve decisions and services?	Provides operational evidence and public-service methods within institutional competence
Legislative Intelligence	How can representative institutions examine, make and oversee law?	Preserves the parliamentary source of norms and scrutiny of the programme
Judicial Intelligence	How can adjudicative institutions improve access, reasons and justice administration?	Maintains independent review and correction rather than becoming an executive analytics module
Fiscal Order Intelligence	How are public resources lawfully raised, authorised, spent and accounted for?	Tests the fiscal legality and sustainability of proposed capability
Sovereign OS	How can these capabilities be organised in an interoperable architecture?	A proposed enabling architecture, not the source of sovereign authority

1.24 These fields can share records and methods without merging their mandates, evidentiary standards or institutional decision rights.

1.25 The institutional framework also shows how the overlapping Intelligence capacities contribute to Sovereign Intelligence. Constitutional Intelligence establishes authority, rights and institutional limits. Legislative Intelligence examines the governing rules and options for reform. Governance Intelligence connects evidence, implementation and correction. Fiscal Intelligence tests resources, commitments and public accountability.

The state-wide question is whether these capacities can be sustained through dependable records, expertise, institutional relationships and control over critical systems.

Three complementary modes

1.26 Evolutionary Legal Intelligence examines how legal and institutional arrangements change, what previous choices produced and how experience should alter current design. Strategic Legal Intelligence compares lawful options, resources, responsibilities and dependencies. Anticipatory Legal Intelligence tests plausible disruptions, secondary effects and future conditions. All three use historical, present and prospective material. Assigning them mechanically to past, present and future would weaken their interaction.

1.27 In a cloud exit, evolutionary analysis asks how the present dependencies accumulated; strategic analysis compares renewal, modular replacement and migration; anticipatory analysis tests loss of identity services or supplier assistance. An earlier successful migration may become irrelevant after a new proprietary component is introduced. In intergovernmental coordination, a stress scenario may reveal that an apparently neutral reporting definition inherited an old exclusion. In source continuity, an anticipated publisher change can make recovery of historical amendments an immediate priority.

1.28 Each use case should contain a short analytical record stating what these modes contributed. A label alone adds little. The useful question is whether a mode changed the evidence sought, the option considered or the risk accepted. Where it changed nothing, reviewers should be able to see why. This prevents the three modes from becoming decorative headings attached to a predetermined recommendation.

International and comparative foundations

International sovereignty, obligations and cooperation

1.29 The international legal starting point is the sovereign equality of states. Article 2(1) of the United Nations Charter places that principle alongside the duty to perform Charter obligations in good faith. Article 2(4) protects territorial integrity and political independence against prohibited threats or uses of force. Article 2(7) addresses intervention by the United Nations in matters essentially within domestic jurisdiction, subject to its stated exception for Chapter VII enforcement. Articles 55 and 56 also place cooperation concerning development and human rights within the Charter framework.[B2]

1.30 For this paper, these provisions establish a relationship between international autonomy and obligation. They support examining how Pakistan can make meaningful choices about its development and institutional capabilities while participating in international cooperation. They provide no automatic answer to whether a particular cloud service, cross-border research arrangement or data-sharing agreement is acceptable. That assessment requires the applicable law, the purpose of the arrangement, the risks it creates and the control available to the participating institutions.

1.31 Human rights law supplies a further foundation. The International Covenant on Civil and Political Rights recognises self-determination in Article 1, requires effective remedies for violations of Covenant rights in Article 2(3), protects against unlawful or arbitrary interference with privacy in Article 17, and guarantees equality before the law and equal protection in Article 26. Article 19 protects expression, including seeking, receiving and imparting information, subject to its terms. These provisions give a legal basis for examining how information practices affect people and their ability to challenge public action.[B3]

1.32 A rights-based account changes the assessment of national capability. An institution's power to gather and combine information must be considered alongside the conditions governing acquisition, use, disclosure and correction. The person represented in a record has interests that persist when the record is moved, linked or

analysed. Errors can affect access to work, benefits, credit, education or legal protection. The ability to identify and remedy such errors is part of the capability that a constitutional state needs to sustain.

1.33 International digital cooperation has increasingly addressed these institutional questions. The Global Digital Compact, adopted as Annex I to General Assembly Resolution 79/1, places digital cooperation within international law and human rights and identifies responsible, equitable and interoperable data governance and international AI governance among its objectives. It also emphasises closing digital divides and building capacity. Its legal character as a General Assembly outcome must be retained when using it to inform national policy.[B4]

1.34 The policy implication is that Pakistan can pursue autonomy through relationships that expand its practical choices. Shared research infrastructure, common technical standards, reciprocal training and collaborative language resources may increase the range of systems domestic institutions can understand and maintain. Such arrangements need explicit terms concerning access, knowledge transfer, jurisdiction, continuity and responsibility. A policy of autonomy must assess how much an arrangement improves the country's ability to choose, including its ability to revise or end the arrangement.

1.35 This approach also recognises unequal capabilities. The cost of advanced computing, specialist expertise and continuing maintenance can make certain strategies impractical within a country's fiscal and energy constraints. The proposed framework therefore evaluates capability against public purposes and sustainable means. The value of a technology investment depends on the function it enables, the people it serves, the dependencies it creates and the commitments required to keep it operating. A national strategy should be able to explain those choices using evidence that can be scrutinised.

Constitutional authority, reasons and public knowledge

1.36 Domestic constitutional law determines which institution may act. The distinction between a state's international position and the powers of its internal institutions becomes decisive when a particular official authorises access to information, signs a contract or relies on an analytical result. The general interest of the state cannot establish the competence of every body acting in its name. Each consequential use of knowledge must be connected to the institution, purpose and procedure through which the relevant power is lawfully exercised.

1.37 The United States Supreme Court's decision in Youngstown Sheet & Tube Co v Sawyer illustrates this requirement. The Court rejected President Truman's asserted authority to seize the steel mills. The majority examined whether the action had a statutory or constitutional basis. Justice Jackson's separate concurrence organised the relationship between executive and congressional authority according to whether Congress had authorised, remained silent about or opposed the action.[B5] The constitutional setting was particular to the United States, but the comparison identifies a question every public technology programme must answer. Which legally competent institution is authorising the action, and from where does its power arise?

1.38 This inquiry reaches decisions that can appear merely technical. Linking databases can expand the persons and activities exposed to scrutiny. A new classification can affect access to a public service. A procurement specification can determine which records an institution will retain and whether those records will be available to a reviewing authority. The legal significance of these choices follows their effects within the public function. Their location in a project plan or software configuration does not remove the need to identify authority and responsibility.

1.39 Lawful authority must also be exercised through defensible reasoning. In Motor Vehicle Manufacturers Association v State Farm, the US Supreme Court held that the agency's rescission of a vehicle-safety requirement was arbitrary and capricious under the governing administrative-law standard. At page 43, the Court explained that an agency must examine relevant data and adequately explain its action. It identified

defects such as overlooking an important aspect of the problem or offering an explanation contrary to the evidence. The same passage cautioned that reviewing courts should respect the proper scope of agency judgment.[B6]

1.40 The contribution of this authority is the relationship it establishes among evidence, expertise, reasons and review. A public institution should be able to show how it moved from material facts and applicable requirements to its chosen course. That account may contain uncertainty and legitimate disagreement. Its purpose is to make the grounds of the decision available for examination. An analytical output becomes useful to the institution when officials can relate it to the question they must decide and recognise circumstances in which it should carry less weight.

1.41 This yields an institutional requirement that the paper proposes as central to Sovereign Intelligence. The records surrounding a significant decision should preserve its legal basis, evidential basis, material alternatives, responsible actors and conditions for reconsideration. A statistical forecast, a professional assessment and a legal interpretation answer different questions. Their contributions should remain identifiable when combined. Otherwise a later reviewer may be able to see the conclusion while being unable to reconstruct the reasoning that produced it.

1.42 Constitutional accountability also requires more than access within the executive. A legislature scrutinising a programme needs information that can reveal failure as well as success. A court reviewing an adverse decision needs the records relevant to the issue before it. An auditor needs to relate expenditure to authorisation, delivery and acceptance. The state-wide capacity proposed here therefore depends on multiple institutions being able to question shared evidence from within their own mandates. Independent scrutiny strengthens the reliability of public knowledge by allowing material errors and disagreements to reach a forum capable of addressing them.

1.43 There is a genuine difficulty in coordinating these capacities. Fragmented records can prevent institutions from understanding the same event. Excessive central control can make access contingent on the interests of the body being examined. The appropriate arrangement depends on the function and legal context, but its design should secure both usable exchange and independent access. Shared standards, defined custodianship and traceable records can assist this work while preserving responsibility for decisions and the lawful limits on disclosure.

Privacy and the constitutional significance of analysis

1.44 Digital systems can change the significance of information through accumulation and inference. Records collected separately for ordinary administrative purposes may disclose much more when combined. A sound legal analysis must therefore examine the use being proposed as well as the original collection. It must also distinguish a fact recorded about a person from an inference made about that person. The latter may depend on assumptions, correlations or incomplete coverage that require their own evaluation.

1.45 In Carpenter v United States, the US Supreme Court held that government acquisition of the historical cell-site location records at issue constituted a Fourth Amendment search. The majority addressed the revealing character of the location history and declined to treat possession by a service provider as conclusive against constitutional protection. It confined the holding and reserved questions concerning other collection practices.[B7] For the proposed framework, the case draws attention to the consequences of aggregation and the legal significance of access to information held elsewhere.

1.46 The Supreme Court of India's privacy judgment in K S Puttaswamy (Retd) v Union of India supplies a complementary constitutional perspective. The nine-judge Court recognised constitutional protection of privacy. The opinion delivered by Chandrachud J for four judges discusses informational privacy and states requirements of legality, legitimate state aim and proportionality for the intrusion under consideration.[B8]

The comparison supports an examination of public information systems that takes purpose, authority and the means chosen together.

1.47 Germany's Federal Constitutional Court has addressed automated analysis directly. In its judgment of 16 February 2023 concerning police data-analysis powers in Hesse and Hamburg, the Court identified automated processing of stored personal information as an interference with informational self-determination. Its published headnotes distinguish the effects of the original collection from the additional effects that automated analysis can produce. They connect justification to purpose limitation, changes of purpose and proportionality.[B9]

1.48 These authorities direct attention to analytical power as a legal and institutional object. A database may be lawfully held while a proposed use raises further questions. A model may generate a new claim about a person without revealing how uncertain that claim is. A search interface may expose information to officials whose functions previously gave them access to a smaller set of records. The institution needs a way to identify these changes before treating greater technical capability as an ordinary extension of existing practice.

1.49 Sovereign Intelligence consequently requires an account of the life of a material inference. Officials should know the question for which it was produced, the sources and methods supporting it, the limitations affecting its use and the process through which it can be challenged. A correlation useful for planning may be unsuitable for determining an individual's entitlement. An incomplete record may justify further enquiry while supplying an inadequate basis for an adverse conclusion. The proposed capacity depends on maintaining these distinctions during actual work.

1.50 Protection of privacy also contributes to public knowledge by making participation more credible. People asked to provide sensitive information need understandable conditions governing its use. Researchers and professional advisers need assurance that lawful confidentiality will be respected. Institutions that seek reliable information must organise the conditions under which it can be entrusted to them. This is a practical governance argument as well as a concern with legal rights. It asks how the state can obtain the knowledge it needs while remaining answerable for its use.

Due process, explanation and correction

1.51 An institution's understanding of a case can improve when the affected person has an effective opportunity to answer it. Administrative records may omit circumstances known only to that person. An identity match may be mistaken. A document may have been supplied through another channel. A rule may have changed after the event represented in the data. The ability to contest a decision is therefore connected to the institution's ability to discover error. It supplies a further route by which public knowledge can be tested.

1.52 In Goldberg v Kelly, the US Supreme Court held that the welfare benefits at issue could not be terminated without the required pre-termination evidentiary hearing. The Court examined the importance of those benefits and the recipient's opportunity to respond to the case for termination.[B10] In Mathews v Eldridge, it reached a different conclusion about a pre-termination evidentiary hearing in the disability-benefit setting. The Court identified three considerations, comprising the private interest, the risk of erroneous deprivation and probable value of further safeguards, and the government's interest and associated burdens.[B11]

1.53 Read together, these decisions support careful design of procedures for particular functions. The requirements of an enquiry about a missing certificate differ from those of a decision that removes an essential source of support. The proposed framework should consider the severity and reversibility of the consequence, the sources of likely error and the affected person's practical ability to obtain correction. A nominal route of appeal has limited value where the person cannot discover the reason for the result or reach someone capable of changing it.

1.54 Automated processing complicates this relationship when a supplier's output strongly determines what follows. In SCHUFA Holding (Scoring), the Court of Justice of the European Union held that an automated credit score could itself constitute automated individual decision-making within Article 22(1) of the General Data Protection Regulation (GDPR) where a recipient relied strongly on it in establishing, implementing or terminating a contractual relationship. The Court examined the gap in protection that could arise if scoring were treated only as a preparatory step.[B12]

1.55 The inference for this paper concerns the actual distribution of judgment. Assessment should follow how an output influences the result. An officer's formal approval may involve real consideration, or it may reproduce a score that the organisation has made difficult to question. Institutions need evidence of which situation exists. Relevant matters include the official's access to underlying information, competence to evaluate it, time to consider the case and authority to depart from the recommendation.

1.56 The Court's judgment in Dun & Bradstreet Austria develops the issue of explanation under Article 15(1)(h) GDPR. It requires intelligible information about the procedure and principles actually used to produce the relevant result. Where disclosure is said to affect protected third-party information or trade secrets, the competent supervisory authority or court must be able to undertake the required balancing.[B13] This supports distinct arrangements for explanation to the individual and protected examination by a competent reviewer.

1.57 For a public institution, such arrangements need to be built into access and procurement decisions. Officials must be able to obtain information relevant to the decisions for which they answer. Reviewing bodies need the access appropriate to their mandates. An intelligible explanation should connect the actual case, relevant evidence, applicable rule and reason for the outcome. A generic account of how a model usually works may leave the decisive issue unresolved. The institution must retain the means to investigate that issue and to implement the correction that follows.

1.58 Correction has a wider institutional purpose. Repeated individual complaints may reveal a defect in a rule, dataset, classification or workflow. The institution should be able to recognise the pattern and determine who can lawfully change the underlying process. A corrected personal record may be insufficient if copies continue to generate the same error elsewhere. Sovereign Intelligence therefore includes the ability to trace the consequences of a correction through connected systems and to preserve the explanation for the change.

Institutional frameworks and the governance of dependencies

1.59 International AI instruments give operational form to several of these concerns. The Recommendation on the Ethics of Artificial Intelligence of the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Recommendation on AI of the Organisation for Economic Co-operation and Development (OECD) address human oversight, accountability, transparency, safety and respect for rights. The OECD instrument also addresses research, capacity building and international cooperation.[B14] Their contribution to the paper is a set of institutional expectations against which a proposed capability can be examined, with the status of each recommendation retained.

1.60 The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law offers a treaty design for a further connection. Articles 4 and 5 address rights, democratic institutions and the rule of law. Articles 14-16 concern remedies, procedural safeguards and risk and impact management. Article 3 treats national security and defence separately and expressly preserves applicable international-law considerations in its national-security provision.[B15] The paper uses these provisions comparatively, with treaty application dependent on the relevant legal conditions and party status.

1.61 The European Union AI Act illustrates how oversight can be specified for particular systems and actors. Article 14 addresses effective human oversight of high-risk systems, including understanding limitations,

guarding against over-reliance and being able to override or interrupt operation. Article 27 requires fundamental-rights impact assessment for specified deployers and uses. Article 2(3) provides the relevant exclusion for exclusively military, defence or national-security purposes.[B16] The provisions should be read within the Regulation's scope and application arrangements.

1.62 Canada's Directive on Automated Decision-Making supplies a public-administration example. Its requirements connect covered administrative decisions to algorithmic impact assessment, notice, explanation and controls scaled to impact. The directive also addresses access to proprietary software for specified audit, investigation and judicial purposes.[B17] Such provisions demonstrate how an institution can make oversight practical through staff responsibilities, access rights and continuing procedures.

1.63 The National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework supplies a complementary voluntary structure organised around governing, mapping, measuring and managing risk.[B18]

1.64 These functions help specify the work needed to understand a system in context. Legal authority and technical assurance remain connected responsibilities. A lawful purpose requires a system suitable for its intended use, while successful testing leaves questions about authority, procedure and remedy to the applicable law and institutions.

1.65 The broader implication is that dependency must be governed through more than ownership. Institutions may rely on contractors for infrastructure, software, analysis and specialist expertise. The arrangement needs to preserve the public body's ability to fulfil its duties. That may require documentation, version histories, access for review, usable exports, incident assistance, training and a credible transition plan. Different functions justify different controls. The terms appropriate for a public information service may be inadequate for a system used to support adverse legal or financial decisions.

1.66 Domestic infrastructure also needs a clear public purpose and durable means. Canada's Sovereign AI Compute Strategy combines public infrastructure, commercial investment and support for access to compute.[B19] It provides an example of several instruments being used toward capability development. For Pakistan, the question is which combination can support the intended workload, institutional users and fiscal commitments. An allocation should be assessable against demand, utilisation, staffing, energy requirements and continuing expenditure. These are proposed criteria for the later policy analysis in this paper.

1.67 There is an objection that this account places too many conditions on urgent technological development. Building expertise and independent review can take time, while institutions face immediate service pressures. The response lies in proportionate scope. A bounded enquiry can establish which records are needed, which decisions a tool will influence and which safeguards must operate before expansion. Some functions can proceed through limited assistance and close supervision. Others require further preparation because the consequences of error are difficult to reverse. The proposed framework asks institutions to make that distinction expressly and fund the capability needed for the chosen course.

Security, secrecy and independent supervision

1.68 National-security functions require a distinct analysis of mandate, sensitivity and oversight. Their need for controlled disclosure creates demanding questions concerning who can examine collection, selection, analysis, sharing and retention. Operational secrecy can be compatible with scrutiny by competent bodies operating under appropriate safeguards. The institutional design must identify those bodies, the information available to them and the authority through which they can address a defect.

1.69 In Big Brother Watch and Others v United Kingdom, the European Court of Human Rights examined bulk interception and identified the need for safeguards across the process. Paragraph 350 addresses assessment of

necessity and proportionality at successive stages, independent authorisation at the outset, supervision and independent review after the event.[B20]

1.70 The judgment supplies a comparative basis for examining controls across an intelligence process, with its Convention setting and particular findings retained.

1.71 An operational dimension appears in the United States' NSPM-11 of 5 June 2026. Within its national-security scope, section 2(c) addresses arrangements to prevent commercial actors or adversaries from disabling, degrading or materially altering mission-dependent AI in the specified circumstances.[B21] This is an example of governing a critical dependency. It raises concrete questions about technical access, approval, continuity and contractual terms, which can be examined separately from the authority to conduct the underlying mission.

1.72 The proposed definition accommodates both dimensions. An institution needs control sufficient to carry out its lawful task, and accountability sufficient to examine the exercise of that task. A capability that fails when a supplier withdraws creates one kind of weakness. A capability whose consequential use cannot reach competent independent scrutiny creates another. Policy must identify the controls appropriate to each weakness rather than allowing the language of sovereignty to conceal the allocation of responsibility.

Pakistan constitutional institutions and the competent actor

Constitutional authority and the distribution of public functions

1.73 The preamble and Article 2A supply Pakistan's constitutional account of sovereignty and entrusted authority. Article 4 makes legality central to the relationship between public power and the individual. Read together, these provisions give the proposed framework a domestic point of departure: the state's knowledge capability must serve authority exercised through the constitutional order.[B27]

1.74 The institutional implication is that every programme needs a sufficiently precise public purpose. Improving administration is an objective, but it leaves open the decisions the programme will support, the persons affected, the records required and the legal powers engaged. An agricultural forecasting service, a taxation assessment and a court-record search system present different questions. Their use of a common model or computing facility does not establish a common legal mandate. The programme's first document should identify the public function and the institution responsible for it.

1.75 Articles 90, 97 and 99 and their provincial counterparts in Articles 129, 137 and 139 establish the relevant executive framework. Article 142 supplies the legislative allocation against which a particular function must be examined.[B28] Sovereign Intelligence should make this allocation visible in the design of a service. A national label can describe scale or ambition. The legal analysis must still identify the subject, the responsible government and the instrument authorising the proposed action.

1.76 A useful distinction is between substantive administration and common technical support. A department may use shared hosting, security monitoring, document retrieval or analytical tools while retaining responsibility for its statutory decisions. The operator of the technical service needs its own authority, responsibilities and access conditions. If it will perform an additional public function, that function requires separate examination. The architecture should make clear when a shared provider is processing information under another institution's instructions and when it is exercising an independently conferred power.

1.77 Federal and provincial cooperation has several constitutional routes. Article 144 concerns legislation following the specified provincial Assembly resolutions. Articles 146 and 147 concern entrustment of functions in different directions and on different conditions, including the provincial Assembly ratification requirement in Article 147.[B29] An implementation agreement should identify which route, if any, is engaged. An

arrangement for exchanging specified records may differ materially from one under which another government will make decisions or exercise administrative powers.

1.78 Such agreements should describe the function being supported, the legal basis for participation, the records involved and the institution responsible for their accuracy. They should identify who can authorise access, change the system, answer a complaint and preserve the evidence of an earlier decision. Financial contributions and additional administrative burdens should be addressed alongside the technical arrangements. These are proposed requirements for dependable cooperation. Their legal form should follow the applicable constitutional and statutory route.

1.79 The Council of Common Interests has an important but defined role under Articles 153 and 154 and Part II of the Federal Legislative List. The National Economic Council under Article 156 provides a distinct forum in economic planning.[B30] Their relevance to a proposed intelligence capability should be established by reference to its subject and purpose. A research-standards question, an interprovincial coordination problem and a department's procurement decision can engage different institutions even when they arise within the same national programme.

1.80 Provincial participation in a coordinating body also needs practical substance. Members require timely documents, an opportunity to examine the evidence, a record of disagreement and a means to determine who will implement the resulting decision. The existence of a forum supplies an institutional opportunity. Evidence of its operation includes the relevant meeting records, decisions, implementation responsibilities and subsequent review. A strategy should be assessed by how these arrangements work for a specific function.

1.81 Local government belongs within the same account. Article 140A provides the constitutional foundation for provincial legislation establishing local government and devolving responsibility and authority.[B31] The actual powers and resources of a local body must be established under the applicable provincial law. A shared system should enable officials to perform those functions with dependable records and accessible procedures. Local knowledge about service delivery, incomplete applications and recurring complaints should also be able to reach the institution capable of changing the process.

1.82 These arrangements favour a distributed institutional model. Each body needs the knowledge appropriate to its responsibilities, while common standards can make records and methods usable across institutional boundaries. Shared capability should be assessed through the lawful work it enables. The design must preserve a traceable connection between the institution holding a power and the person or system carrying out the relevant task.

Government business and the chain of authorisation

1.83 Rules of Business give operational form to executive responsibility. The Cabinet Division's published federal compilation is amended up to 28 September 2026. Its consultation and Cabinet-procedure provisions help identify how proposals involving several divisions, public money or legal instruments should move through government.[B32] A technology programme should be mapped against that process before specifications and contracts begin to determine its institutional shape.

1.84 An authorisation record needs to distinguish the stages a project passes through. An expression of policy support, approval to explore an option, permission to spend, authority to procure and acceptance of a delivered system are different events. The record should show what each decision permits and the conditions attached to it. An officer considering expansion must be able to establish whether the original approval covered the new use, users, datasets or recurring commitments.

1.85 The federal Rules address consultation with the Finance Division, the Law and Justice Division and other divisions in the situations they specify. Rule 16 identifies classes of business for Cabinet consideration.[B33]

These requirements connect different forms of expertise to the government's decision. A financially viable proposal may still require a new legal power. A legally available option may require funding and administrative capacity that the sponsor has not secured. An implementation plan should make those dependencies examinable before commitments become difficult to reverse.

1.86 The Supreme Court's decision in Mustafa Impex places the identity of the competent government at the centre of this inquiry. The Court allowed the appeals and struck down the challenged fiscal notifications, examining the constitutional description of the Federal Government and the required business procedure.[B34] For Sovereign Intelligence, the relevant lesson concerns accurate attribution of power. A proposal must identify who holds the function, the procedure governing its exercise and any lawful authorisation under which another actor may perform the task.

1.87 The later decision in Government of the Punjab v Zaka Ullah applies this reasoning in a provincial regularisation dispute involving posts, expenditure and governmental approval. The Supreme Court allowed the appeal and set aside the High Court's direction in the circumstances before it. Its reasoning examines the required Cabinet and financial approvals and the applicable Rules of Business.[B35] The case supports careful treatment of staffing and expenditure within a capability programme, while retaining the particular statutory and administrative context.

1.88 The resulting design should allow routine work to proceed through valid arrangements while preserving responsibility for consequential changes. It should identify who can approve a new data source, change an eligibility rule, accept an analytical method, authorise a material contract variation or suspend a defective system. A standing committee or project team can coordinate preparatory work. Its recommendations need to reach the actor empowered to decide. Where a function is delegated or otherwise authorised, the instrument, scope and conditions should be retrievable.

1.89 This makes the record of authority a continuing operational asset. It should be maintained alongside technical documentation and updated when laws, portfolios, delegations or institutional structures change. A platform can preserve links to these instruments, but legal officers must examine their effect. A system that displays an obsolete allocation confidently can create institutional confusion precisely when staff assume the legal question has already been resolved.

1.90 The cited sources contain a concrete example. Rule 16(1)(e) and Schedule V-B item 54 in the September 2026 federal Rules of Business compilation retain a Supreme Court advisory-reference entry citing Article 186. The cited constitutional consolidation records Article 186 as omitted and provides the Federal Constitutional Court advisory route in Article 175H. The Constitution controls over an inconsistent subordinate procedural reference. Neither entry should be relied on as an operative route without examination of the controlling provisions and any corrective instrument. The date on a compilation cannot by itself establish that every embedded legal reference has been reconciled. The comparison uses the September 2026 Rules compilation and the cited constitutional consolidation; no corrective instrument is established by the sources cited here.[B33]

Rights, evidence and the reasoned public decision

1.91 The rights provisions relevant to a particular use include Articles 4, 8, 10A, 14, 19A and 25, each with its own terms and scope.[B36] They provide the constitutional questions against which a proposed information practice should be examined. The institution must consider the decision being made, the interests affected and the applicable procedure. A general commitment to responsible AI acquires practical meaning through those questions.

1.92 An affected person needs a usable account of a consequential decision. That account should identify the issue decided, the applicable requirement, the material evidence and the reason for the result. It should distinguish

missing information from evidence that a condition is not satisfied. It should also identify the route for correcting a record or challenging the conclusion. These are proposed design requirements whose legal implementation must follow the relevant function and governing procedure.

1.93 Pakistan's own administrative case law supplies an important foundation. In Muhammad Amin Muhammad Bashir Ltd v Government of Pakistan, the Supreme Court examined the evidential basis and reasoning supporting a customs valuation decision and remanded the matter for fresh determination. The judgment connects statutory discretion with relevant evidence and distinguishes review of the decision-making process from the administration's technical task.[B37]

1.94 The decision illustrates a domestic requirement for examining evidence in its statutory setting. Data must be suitable for the legal question the institution is deciding.

1.95 A model can be statistically accurate against a benchmark while relying on information that is out of date for the case before the official. A record can be correct in its original setting while unsuitable for a new inference. A high-confidence identity match can still require investigation where the consequences are serious and a person disputes it. Institutional evaluation should therefore examine the relationship among the governing rule, the date and provenance of the evidence, the analytical method and the decision the official is required to make.

1.96 The federal Right of Access to Information Act 2017 connects access with record maintenance, proactive publication and designated responsibilities, while also providing exclusions, exemptions and an appeal structure within its scope.[B38] This is relevant to the organisation of Sovereign Intelligence before a request is received. A body cannot reliably disclose, examine or correct records that it has failed to preserve or locate. The administrative system needs to identify the authoritative record and the official responsible for responding.

1.97 The Supreme Court's decision in Mukhtar Ahmad Ali v Registrar, Supreme Court demonstrates why the legal route matters. The majority distinguished the reach of the federal information Act from Article 19A and ordered specified information to be supplied. It did so while rejecting the particular statutory jurisdiction asserted over the Court.[B39] The case supports information accountability designed for the institution concerned. It requires the paper to preserve the relationship between a constitutional right, the statute implementing access and the body competent to consider a complaint.

1.98 Publication and privacy also require differentiated handling. An institution may publish service requirements, legal instruments, methodology and aggregate results while protecting personal case material under the applicable law. A reviewing authority may need access to information that cannot lawfully be published generally. The system should support these distinctions through access rules, records of disclosure and reasoned decisions. A single permission setting labelled public or confidential is unlikely to capture the different functions involved.

1.99 Participation can improve the evidence on which an institution relies. Service users may identify a repeated document demand, a language barrier or a mistaken classification that administrative metrics have missed. Professional organisations and researchers may expose a weak assumption in an analytical method. The institution should establish how such information enters the decision process, who assesses it and how a material correction reaches those responsible for implementation. The value of participation depends partly on whether the organisation can act on what it learns.

Parliament, courts and independent examination

1.100 Sovereign Intelligence includes the capacity of institutions that examine government action. Parliament requires evidence concerning a programme's authority, expenditure, performance and consequences.

Members need to understand what has been delivered, which groups encounter difficulty and what the implementing body proposes to do about failure. Data should be accompanied by definitions, time periods and explanations sufficient to make comparisons intelligible.

1.101 The National Assembly's Rules of Procedure and Conduct of Business, in the compilation amended to 18 August 2026, provide for committee examination of referred matters and powers concerning evidence and records, with the qualifications specified in the Rules. Rule 226 addresses meetings in camera and Rule 227 the production of evidence and documents.[B40] These provisions support scrutiny through procedures suited to the material concerned. Sensitive information should be addressed through the applicable process, with the institution's access needs and legal safeguards examined together.

1.102 An executive dashboard is one source of information for scrutiny. Parliamentary work also requires the ability to question classifications, obtain underlying material where authorised and examine the assumptions used to declare a programme successful. A report showing completed transactions may omit people who could not begin an application. A measure of expenditure may reveal little about whether the service became dependable. The parliamentary evidence package should therefore distinguish activity, outputs, outcomes and unresolved problems.

1.103 Judicial review requires an equally careful institutional map. The cited constitutional consolidation includes the Federal Constitutional Court and the jurisdictions addressed in Articles 175E and 175F alongside Article 199 and the constitutional-bench arrangements in Article 202A. The latter's activation conditions must be considered for the relevant High Court.[B41] A programme should identify the forum and procedure applicable to its decisions when designing preservation, disclosure and compliance arrangements.

1.104 For that purpose, the decision record should preserve the rule and system version used at the relevant time. A later update may improve performance while leaving a dispute about an earlier decision unresolved. The institution needs the ability to reconstruct what occurred, identify the evidence available then and explain the action taken. Contracts and retention arrangements should make that reconstruction possible for the period required by the applicable legal regime.

1.105 The Digital Nation Pakistan Act contains an express jurisdiction-bar provision in section 29. Its constitutional reach must be examined alongside the Constitution and relevant judicial authority.[B42] The institutional design should identify a defensible route for reviewing the particular exercise of power. An internal grievance arrangement, a statutory appeal and a constitutional application perform different functions. The existence of one process should be examined against the legal requirements governing the others.

1.106 Independent examination also needs its own expertise and information access. Courts, audit offices, parliamentary committees and specialist complaint bodies may require technical assistance to understand records and analytical methods. That assistance should support the institution's judgment and preserve its independence. A national strategy should identify how such expertise will be available, who will maintain the relevant records and how the cost will be sustained. Oversight capacity belongs in the capability plan from its beginning.

Digital institutions within the constitutional order

1.107 The Digital Nation Pakistan Act 2025 gives the national programme a statutory institutional structure. Sections 3-5 establish the National Digital Commission and its planning role. Sections 6-8 concern the Pakistan Digital Authority, while sections 9-10 establish an Oversight Committee with specified review and reporting functions.[B43] These institutions supply identifiable places in which strategy, coordination, delivery and evaluation can occur.

1.108 Their legal relationship with the institution performing a public function remains central. Section 8(g) ties the Authority's AI-related functions to areas assigned by the Commission and addresses regulatory overlap and conflict with laws. Section 8(h) preserves designated custodians' control and responsibility for datasets.[B44] Those provisions make the actual assignment, the relevant sector law and the data-custody arrangement important evidence in assessing a particular programme.

1.109 A service-level institutional map should consequently identify several actors. The body holding the substantive power needs to retain an intelligible decision procedure. The custodian needs to preserve the identity and quality of the relevant source records. The technical operator needs defined responsibilities for processing, security and continuity. A regulator or reviewing body needs the access appropriate to its jurisdiction. The same organisation may perform more than one role, but each responsibility should be recorded distinctly enough to identify who must act when a problem arises.

1.110 The statutory Oversight Committee's functions and conflict-of-interest provisions should be examined within that structure.[B45] Its reviews can contribute to programme assurance. The wider accountability system also includes the institutions competent to examine legality, public expenditure, access and individual complaints. Each review should state the question examined, the evidence available, the conclusion reached and the person responsible for following it through. Approval by one body should be recorded according to its actual legal and evidential significance.

1.111 The Masterplan and implementation arrangements under sections 11-12 provide a further set of operative documents to examine.[B46] A department needs to know which approved plan applies to it, which directions have been issued, what outcomes it is expected to produce and how compliance will be assessed. The approved instrument and its version should be accessible to officials who must implement it. Changes should be recorded with their effect on existing projects, commitments and service users.

1.112 Information powers require particular care. Section 19 addresses assistance and information, while section 28 expressly addresses protective laws concerning data rights and cybersecurity.[B47]

1.113 A request for records should be connected to its statutory purpose, the information actually needed, the recipient's handling responsibilities and the applicable protections. Technical access should implement the lawful arrangement reached through that analysis. The creation of a data-exchange facility does not by itself settle every question about what may pass through it.

1.114 Delegations, rules, regulations and policy directions under sections 24-27 require attention to the particular instruments and their publication requirements.[B48] A functioning register should identify the source of a claimed power and the date from which it operates. It should connect an amendment or withdrawal to the systems and workflows affected. This is one practical contribution an institutional knowledge service can make: enabling officials and reviewers to recover the instruments governing a decision at the relevant time.

1.115 The National AI Policy 2025 describes a further policy structure, including an AI Council and a Policy Implementation Cell. The Islamabad AI Declaration supplies principles on accountability, capability and coordinated governance.[B49] The relationship between those policy arrangements and the statutory Commission, Authority and other institutions should be established through the instruments actually issued. A programme needs a clear account of who sets priorities, who provides implementation support, who exercises a legal power and who evaluates the result.

1.116 The Islamabad AI Declaration provides a policy connection through its principles on human accountability, data stewardship, auditable systems, coordinated governance, capability and sovereign compute. The National AI Policy 2025 sets out a wider programme across innovation, readiness, security, transformation, infrastructure and international partnerships.[B26] Their implementation should be assessed through the instruments, expenditure, operating arrangements and observed outcomes relevant to each commitment.

A public-accountability chain rather than a command pyramid

1.117 The proposed chain begins with the public purpose and ends with an intelligible account of what happened. Between them lie competence, source evidence, institutional judgment and a record that can support scrutiny. The chain is not a hierarchy in which every participant reports to the analytical system. It is a sequence of obligations that the system should help the responsible institutions discharge.

Element	Question the record must answer	What technology cannot supply by itself
Public purpose	Which public problem is being addressed, for whom and with what exclusion risk?	Democratic legitimacy from usage counts
Competence	Which institution may perform this particular action?	A power absent from the applicable legal route
Evidence	Which source, version and transformation support the proposition?	Legal currency merely because retrieval succeeded
Judgment	Which assumptions and alternatives were assessed by the responsible office?	Adoption merely because a model recommends an option
Consequence	Which authorised act, if any, follows the analysis?	A spending, disclosure or enforcement power
Accountability	How can the decision be scrutinised, corrected and, where appropriate, challenged?	Remedy merely by displaying a complaint button

1.118 A useful control record names the institution and office before naming the model. In the cloud case the service owner is responsible for continuity, while the procurement and expenditure routes remain distinct. In the federation case each participant's information route and competence survive a shared options dossier. In the legal-memory case a research answer remains distinguishable from an authoritative institutional act. These separations are not obstacles to coordination. They make coordination intelligible and defensible.

A developed parliamentary and executive briefing workflow

1.119 Consider a constructed request for a joint factual briefing on public-information continuity. The question is whether essential information remains available when a primary supplier fails. The analyst creates one evidence package containing scope, source manifests, test results, unresolved dependencies and the illustrative cost comparison. A recipient manifest then identifies which material may be included in a parliamentary scrutiny brief, an executive implementation brief and a public summary. Restricted configurations and protected records are not copied into the public version simply because the analytical conclusion is public.

1.120 The parliamentary-facing brief asks what was promised, what was tested, what failed, which resources were used and what remains uncertain. The executive-facing brief identifies the responsible offices, dependencies to correct, lawful next steps and the decision deadline. Neither version alters the underlying failure record. If an executive office requests a more favourable summary, the workbench preserves the evidence and records the proposed change rather than silently converting a failed test into a success.

1.121 An output status of ready for briefing means only that the package meets its defined evidence and review checks. It does not mean that a House has considered it, that the Cabinet has adopted it or that a contract may be signed. A receipt records transmission to an authorised recipient; an institutional decision record separately records any subsequent act. This is the basic architecture for bringing Prime Minister House, the Presidency and Parliament into the analysis without conflating their roles.

Public Judgment Reasons and Accountable Reliance

1.122 The exercise of public power requires an institution to move from information to a judgment for which it can answer. A statistical pattern, a professional opinion, a prediction and a finding of legal entitlement each contribute differently to that process. The question for Sovereign Intelligence is how knowledge can improve public action while preserving the authority, reasoning and procedures through which that action becomes lawful and justified. The quality of an intelligence capability must therefore be examined in the decisions it enables and in the means available to challenge and correct them.

1.123 The argument concerns a capacity that extends beyond AI. A department can adopt an unexplained consultant's recommendation, an inherited administrative formula or an unsupported professional assumption just as it can adopt a computational score. Each arrangement raises questions about authority, evidence and responsibility. AI makes some questions more pressing by increasing the scale and speed of analysis and by introducing additional dependencies between the institution, the method and the source of its information. The legal enquiry should identify the actual relationship rather than assume that the technology's name resolves it.

1.124 The chapter's central proposition is that the acceptability of an intelligence system should be assessed through the public function it supports, the consequences of its use, and the institution's ability to justify, review and correct the resulting action. This is a proposed evaluative position for the paper. The applicable law supplies the enforceable duties in a particular setting. Academic arguments and comparative authorities help test the position and identify where additional policy commitments may be justified.

Public Judgment within the Constitutional Order

1.125 Pakistan's constitutional starting points remain legality, the distribution of public authority and the rights engaged by its exercise. Article 4 concerns treatment in accordance with law; Article 10A addresses fair trial and due process in determining civil rights and obligations or a criminal charge. Articles 14, 19A and 25 contribute further questions concerning dignity, information and equality within their respective terms.[B82] These provisions should direct attention to the person affected as well as the institution administering the function. The design of a decision process must make the applicable requirements practical.

1.126 Authority and knowledge perform different work. An institution may possess relevant expertise while lacking power to determine the matter. A body holding the power may need assistance to exercise it competently. Sovereign Intelligence should connect the two without obscuring which institution is responsible for the decision. A source of advice acquires no additional public competence merely because its advice is sophisticated, widely used or procured under a government contract.

1.127 The significance of the legally competent actor was examined in the constitutional and institutional analysis through Mustafa Impex. The Supreme Court's reasoning concerned the constitutional identity of the Federal Government and the fiscal notifications before it.[B83] Its relevance here is an institutional discipline: identify the source of power, the actor entitled to exercise it and the process required for the particular action. The case does not make every administrative step a Cabinet decision. Its application depends on the relevant power and the operative legal arrangements.

1.128 An intelligence-assisted process should accordingly distinguish advice, verification, recommendation and determination. A tool may identify a possible inconsistency in a record. An authorised officer may seek further information. A designated authority may then decide whether the governing condition is satisfied. The institution should establish which of these acts has legal consequences and whether any responsibility can lawfully be delegated. Describing the whole sequence as a single automated service can conceal distinctions that determine both validity and remedy.

1.129 Section 24A of the General Clauses Act 1897 supplies a further statutory reference in the settings it governs. It addresses reasonable, fair and just exercise of a power conferred by an enactment, advancement of its purposes, reasons to the extent necessary or appropriate, and provision of the order or direction to the prejudicially affected person.[B84] Its scope and qualifications matter. The provision should be applied through the relevant enactment and institutional setting, with attention to applicable provincial provisions. The paper's broader policy recommendations should remain distinguishable from the precise statutory duty.

1.130 The relationship also runs from law to the definition of the problem. A prediction that an applicant resembles people previously refused assistance does not establish that the applicant fails the present entitlement conditions. A forecast of administrative cost does not by itself determine whether a right may be restricted. A legal framework can require the authority to consider a fact that historical data record poorly. The institution must establish the question it is authorised to answer before deciding what information or analytical method can assist.

1.131 An objection is that institutions necessarily depend on expertise they cannot reproduce internally. A regulator cannot repeat every scientific study, and an administrator cannot personally reconstruct every statistical method. That objection is substantial. Responsible reliance should be examined through the quality, relevance and limits of the advice, the means of obtaining clarification and the safeguards appropriate to the consequence. The appropriate institutional capacity is to recognise when specialist assistance is adequate and when further enquiry or independent examination is required.

Evidence, discretion and the treatment of uncertainty

1.132 Public judgment requires a connection between the applicable legal question and the evidence used to answer it. Information can be accurate yet irrelevant to that question. It can be relevant but outdated, incomplete or too uncertain to carry the proposed inference. An apparently precise conclusion can depend on definitions or assumptions that the decision-maker has never examined. A competent process should identify the proposition for which each important item is relied on and the limits of that reliance.

1.133 In Muhammad Amin Muhammad Bashir Ltd v Government of Pakistan, the Supreme Court examined customs valuation, structured discretion, relevant evidence and the distinction between review of the decision-making process and redetermination on the merits. It remitted valuation to the responsible administration.[B85] The judgment's significance for this paper lies in the relationship between legal purpose, the suitability of evidence and a reviewable exercise of discretion. Its customs setting should be retained. It supplies no universal evidential formula for every public decision.

1.134 The institution should distinguish an observed fact, an inference from facts and a prediction about a future event. A record showing that an address was entered on a particular date establishes something different from proof of residence throughout a later period. A group-level association establishes something different from the conduct of a particular person. Where an inference affects a legal position, the responsible authority should explain the bridge from the source material to the conclusion and consider material evidence that challenges it.

1.135 Uncertainty should be represented in a way that informs action. A numerical confidence estimate can be useful, but its legal relevance depends on the question and on the assumptions behind it. Some decisions can proceed on provisional information because delay would create serious harm and later correction is available. Others require stronger evidence before the state acts. The governing law determines the applicable threshold and procedural protections. The programme should identify those requirements rather than translate every question into a common numerical cut-off.

1.136 Discretion adds a further dimension. A statute may permit the authority to weigh several considerations, distinguish unusual circumstances or choose between lawful responses. A fixed recommendation can assist

consistency, but the institution should determine whether treating it as conclusive would suppress a consideration the law requires. Where exceptions are available, staff need the competence and practical means to recognise and examine them. An exception process that cannot alter the outcome supplies little protection to the person whose circumstances fall outside the ordinary pattern.

1.137 Consistency is nevertheless a serious public value. Similar cases should be examined under stable and publicly defensible criteria, and unexplained variation can conceal favouritism or error. The response is to organise discretion through relevant criteria, reasoned distinctions and records capable of review. A departure should be justified where the applicable process requires it. Equally, an institution should be able to explain why a recurring recommendation remains appropriate when an applicant presents credible contrary evidence.

1.138 The United States Supreme Court's reasoning in State Farm provides a useful comparative expression of the relationship. Within the federal administrative-law standard it applied, review was narrow, while the agency remained responsible for considering relevant material and explaining its choice. The reviewing court could not supply a basis the agency had failed to give.[B86] The analogy supports examination of an institution's actual reasons while preserving the respective functions of administration and review. It does not import the American statutory standard into Pakistani law.

1.139 The temporal record is particularly important where knowledge changes. An institution should be able to establish what information was available when it acted, what further information could reasonably have been obtained and what a later discovery changes. A subsequent improvement in a model does not establish that an earlier decision was lawful. A later correction does not by itself prove that the original officer acted improperly. Responsibility must be assessed against the relevant duty, evidence, process and time.

Reasons, participation and the person affected

1.140 Reasons connect public authority to the person whose position it determines. They can identify the applicable rule, the material facts, the inference drawn and the basis for resolving a disputed issue. They can also show why an apparently relevant submission was rejected. The required form and extent depend on the governing law and the decision concerned. The proposed policy objective is that a consequential decision should reach its addressee in a form that makes the available opportunity for challenge usable.

1.141 Jerry Mashaw's account of reasoned administration supplies an academic foundation for this relationship. He examines reasons as part of the different relationships among administrators, supervising institutions and the public, and connects reason-giving with democratic legitimacy. He also recognises practical limits to judicial enforcement and the contribution of internal and other supervisory arrangements.[B87] His comparative account supports attention to both the addressee and the institutional setting. It is a scholarly argument, rather than a source of a general Pakistani right to reasons.

1.142 The paper proposes that reasons be assessed for their connection to the actual decision. A statement can be fluent and detailed while failing to identify the ground on which the authority acted. A generic paragraph about public interest may leave the decisive fact undisclosed. A model-generated narrative can present a plausible account without establishing that it describes the process followed. The institution should preserve and communicate the basis actually adopted, to the extent and through the procedure the law requires.

1.143 This creates a distinction between explaining a system and justifying an action. A technical account may describe the operation of a method. A case explanation may identify the inputs and considerations affecting an output. Legal justification must connect the public action with the applicable authority, relevant evidence and permissible grounds. These accounts can assist one another, but their adequacy must be assessed against the question each is intended to answer.

1.144 Participation contributes information as well as procedural protection. The person affected may know that an address is obsolete, that a transaction was reversed or that two records concern different people. An opportunity to respond can reveal an error that a more elaborate analysis of the same incomplete data would reproduce. The process should identify when representations must be received, who considers them and how they can affect the decision. A notice issued after an irreversible consequence may provide a materially different protection from a timely opportunity to be heard.

1.145 The comparative relationship between Goldberg v Kelly and Mathews v Eldridge is instructive. Goldberg required a pre-termination evidentiary hearing in the welfare setting before it. Mathews considered the different disability-benefit process and articulated a contextual balancing enquiry concerning the interest, risk of error, value of safeguards and governmental burden.[B88] The decisions demonstrate the need to examine the particular procedure and interests. They establish neither a single hearing format for every benefit decision nor a Pakistani rule governing automated administration.

1.146 Administrative scale presents a genuine difficulty. Institutions may decide thousands of matters under common rules, and requiring an elaborate individual explanation at every stage can divert resources from timely service. Proportionate forms can include clear standard reasons linked to the actual ground, identification of the disputed information and an accessible route for further explanation or review. The adequacy of such arrangements depends on the legal requirements and on whether they work for the person receiving them. Standardisation should preserve the ability to identify a case that needs individual examination.

1.147 The same enquiry must address language, disability, connectivity and access to assistance. A formally available challenge can be difficult to exercise when the notice is incomprehensible or the relevant evidence cannot be supplied through the offered channel. A service should identify the people likely to encounter these barriers and provide appropriate routes within its responsibilities. The objective is a procedure through which a material objection can reach a person or body capable of deciding it.

Academic arguments about opacity and institutional responsibility

1.148 Academic analysis helps identify competing accounts of what accountability requires. One account emphasises access to the grounds of a decision and the capacity of the person affected to challenge them. Another asks which institutional arrangements can establish that a method observes the relevant requirements. A further position favours the use of inherently interpretable methods in consequential settings. These arguments address related concerns, but they can produce different recommendations about disclosure, system selection and the role of independent examination.

1.149 Danielle Keats Citron's account of technological due process examines how automated administration can combine individual adjudication with policy choices embedded in a system. Her proposals include meaningful notice, records of the facts and rules used, protection against uncritical reliance, and procedures addressing the policy choices underlying repeated decisions.[B89] This moves the enquiry beyond an isolated appeal: the institution may need to examine a recurring practice that generates many outcomes. Her account also recognises the potential benefits of automation. It should be read as an argument for reconstructed procedural protection, within its American administrative-law setting.

1.150 For Pakistan, the analytical implication is that an individual challenge and a system-wide enquiry should be able to inform one another. An applicant may establish a factual error in a single case. A reviewing institution may then discover that the same erroneous rule or source affects a wider set of decisions. The institutional response should identify who can examine that wider issue and what legal powers support corrective action. The procedural demands remain anchored in the applicable domestic framework.

1.151 Jenna Burrell distinguishes opacity arising from intentional secrecy, specialised knowledge and the characteristics and scale of machine-learning methods. She argues that identifying the forms involved helps select an appropriate response.[B90] The distinction supports a more precise enquiry than asking whether a system is simply transparent. Disclosure may address a withheld document, training may address a knowledge gap, and another kind of examination may be needed where complexity limits interpretation. These possibilities still require assessment against the task and the information needed for lawful review.

1.152 Cynthia Rudin advances a stronger preference for inherently interpretable models in high-stakes decisions. She questions explanations produced separately from an opaque model and challenges the assumption that improved accuracy necessarily requires sacrificing interpretability.[B91] Her position deserves consideration when an institution claims that opacity is unavoidable. It calls for examination of available alternatives and of the evidence behind a claimed advantage. The article's examples and arguments do not establish the performance of any proposed Pakistani deployment, and its scholarly prescription is distinct from a binding domestic rule.

1.153 The strongest objection to a contextual approach is that institutions may repeatedly describe opaque systems as indispensable without seriously testing alternatives. A case-by-case formula can become a means of avoiding a principled limit. The response should therefore require a documented comparison proportionate to the consequence, identify any applicable non-negotiable legal conditions, and place responsibility for the choice with the competent public body. Contextual reasoning should produce grounds capable of examination, including grounds for refusing the proposed use.

1.154 There is a corresponding objection to requiring complete public disclosure in every setting. It may expose personal information, compromise a legitimate protective operation or provide material that few people can interpret. The proper enquiry is what information and access the relevant procedure requires, who should receive them and how competing interests are lawfully resolved. An institution must assess whether a controlled arrangement supplies adequate scrutiny or leaves an essential question inaccessible. A general appeal to secrecy cannot perform that assessment.

1.155 The paper's synthesis is an institutional account of justification. Interpretable methods, meaningful explanations, evidence of suitability and independent scrutiny can each contribute to accountability. Their contribution depends on the function and on the rights and duties engaged. Where the applicable law requires a particular explanation or opportunity for challenge, a policy preference for efficiency cannot remove it. Where the law leaves room for institutional design, the proposed safeguards should be justified through the public purpose and the consequences of error.

Assessing black-box intelligence in context

1.156 The expression black-box intelligence should identify a question for examination rather than settle the answer. The institution should specify what is unknown, to whom it is unknown, why that information matters and whether the gap can be addressed. A user may lack specialist knowledge that an independent examiner possesses. A supplier may withhold material it could disclose under controlled conditions. A method may be difficult to interpret even when its design is available. The safeguards needed in these situations can differ.

1.157 The proposed enquiry begins with the system's actual influence. A search tool that helps an officer locate a document plays a different role from a score that effectively determines which applications are rejected. The label advisory should be tested against workflow, staff authority, available time and the treatment of disagreement. A recommendation can become decisive in practice when the official cannot inspect its basis or depart from it without facing an unexplained institutional penalty.

1.158 Consequence and reversibility also matter. An error in a provisional forecast may be addressed through updating and professional interpretation. An error that deprives a person of essential assistance or contributes

to coercive action can require stronger safeguards before the action occurs. The assessment should consider the seriousness, distribution and duration of harm, the possibility of independent verification and the ability of those affected to initiate a challenge. It should also examine the proposed alternative, including its errors and burdens.

1.159 The following distinctions express a proposed policy approach. They are hypothetical applications of the chapter's argument, subject to the governing law and evidence for the actual use.

Role of an opaque system	Principal public-law concern	Proposed institutional response
Research assistance or document discovery	Inaccurate sources or omissions influencing professional work	Require source checking and retain the professional's responsibility for the proposition adopted.
Forecasting used in planning	Uncertainty, unsuitable assumptions or unequal consequences of resource allocation	Examine the method's suitability, alternatives, limitations and the reasons for the resulting policy choice.
Selection, prioritisation or individual assessment	An apparently preliminary output effectively determines treatment or entitlement	Examine actual influence, relevant criteria, information available for challenge and independent decision-making capacity.
Adverse legal determination or support for coercive action	An essential ground cannot be examined or contested under the required procedure	Establish the applicable legal threshold and disclosure duties; restrict or suspend the proposed use where its deficiencies cannot be remedied.

1.160 Comparative cases demonstrate the importance of retaining the actual legal setting. In State v Loomis, the Wisconsin Supreme Court affirmed the denial of resentencing and permitted consideration of COMPAS within specified limits. Scores could not determine incarceration or sentence severity, or be determinative of safe community supervision; independent factors had to support the sentence.[B92] The decision is a conditional sentencing ruling. It neither certifies scientific reliability nor establishes an unrestricted permission to use proprietary systems in other public functions.

1.161 In SCHUFA, the Court of Justice of the European Union examined an automated creditworthiness score under Article 22 of the GDPR. Where the score played the determining role described by the referring court, its production could itself fall within the relevant concept of a decision.[B93] The lesson for the proposed framework is to examine practical influence. This is a comparative inference from a particular data-protection regime, including its exceptions and safeguards; it is not a directly applicable Pakistani prohibition.

1.162 In CK v Dun & Bradstreet Austria, the Court addressed intelligible information about the procedure and principles actually applied in automated processing. Where protected third-party information or trade secrets were invoked, the competent authority or court had to receive the information and balance the relevant interests.[B94] The judgment supports a distinction between an intelligible account and an unexplained formula. It also illustrates structured treatment of confidentiality within the GDPR, without requiring universal public disclosure of source code.

1.163 The institution should avoid treating a generally successful performance record as proof of suitability for every row. Different questions require different evidence. Aggregate performance may leave a material group poorly served or conceal an error type whose consequences are especially serious. The person challenging an individual decision may need information that a population-level evaluation cannot supply. A defensible assessment should connect the evidence of capability to both the intended function and the available procedure.

1.164 Confidentiality requires similarly specific examination. Trade secrets, personal information and legitimate operational security can justify restrictions under the applicable law. The institution should identify the material protected, the legal basis for protection, the person seeking access and the review arrangements available. Possibilities include disclosure of an intelligible case explanation, controlled access for an expert or examination by a competent independent body. Their adequacy depends on what the affected person must be able to know and challenge.

1.165 The public body should address these questions when selecting the service. If a foreseeable dispute will require access to information the supplier refuses to preserve or provide, the proposed arrangement contains an institutional defect before the first case is decided. Procurement should secure the assistance and access needed to discharge the body's responsibilities. A supplier's terms cannot by themselves determine the extent of a public authority's legal obligations.

1.166 Case-by-case assessment therefore permits several outcomes. A use may be supportable under defined conditions, suitable for a limited purpose, dependent on further evidence or inappropriate for the intended function. The assessment should state which conclusion follows and why. It should identify conditions that would require reconsideration, including a change in purpose, decisional influence, affected population or access for review. This makes contextual assessment a reasoned institutional practice.

Judicial assistance and independent legal judgment in Pakistan

1.167 Judicial uses require attention to the nature of adjudication and the applicable institutional arrangements. Research assistance, scheduling and preparation of an initial summary can support a court's work. Determination of the issues, evaluation of the parties' submissions and adoption of the reasons belong within the judicial responsibilities established by law. The fact that material is presented in the form of a draft judgment does not establish that the necessary adjudicative work has occurred.

1.168 In Ishfaq Ahmed v Mushtaq Ahmed, the Supreme Court allowed an appeal in a rent dispute and also developed substantial observations on judicial AI. Paragraphs 9 and 11-13 emphasise assistance, verification and independent judicial responsibility; paragraph 18 recommends institutional guidelines.[B95] The AI discussion should be distinguished from the tenancy reasoning and operative eviction disposition. Its treatment here concerns judicial responsibility, without adopting every empirical or philosophical proposition in the discussion as an independently established fact.

1.169 Pakistan's National Guidelines for Use of Artificial Intelligence in Judicial Institutions are a concrete reference. Clauses 4.1-4.2 address independent judicial reasoning, transparency, identification of generated portions and verification. Clause 5 lists assistance uses, while clause 5.5 expresses a preference for locally developed explainable systems trained on Pakistani legal data. The National Judicial (Policy Making) Committee adopted them at its 57th meeting on 11 February 2026; issuance was announced on 29 April 2026.[B96] Clause 3.2 makes implementation subject to applicable law and High Courts retain autonomy over local arrangements; the contextual approach here cannot displace an applicable requirement.

1.170 The listed predictive applications concern case duration and patterns for resource allocation and management. The institution should distinguish those purposes from an assessment that affects the merits of a dispute. Even an administrative use can acquire consequential influence: prioritisation may affect when a person can obtain relief, and a deficient summary may conceal a material submission. The relevant enquiry concerns what the assistance changes in the proceeding and how that change is examined.

1.171 Judicial independence also requires professional independence from a supplier's conclusions and from an unsupported generated account of authority. A judge or legal professional should be able to recover and examine the source relied on, distinguish the holding from commentary and consider material contrary authority. The appropriate procedure for addressing generated or assisted material should preserve the parties'

rights and the court's responsibility under the applicable rules. Publication of polished reasons must be connected to the legal reasoning and consideration the proceeding requires.

Responsibility, independent review and effective correction

1.172 Accountability requires an identifiable institution with the duty and practical capacity to respond. An explanation of how responsibility is divided among a department, a shared operator, a professional adviser and a supplier should enable an affected person or reviewer to find the competent body. Internal complexity should be addressed through the allocation of work and records. A person seeking correction should receive a route through that arrangement that corresponds to the governing procedure.

1.173 Human involvement contributes only what the human participant is equipped and authorised to do. An official needs sufficient information, relevant competence, time and a route for resolving uncertainty. The ability to disagree should be practical and recorded. A signature can establish that an official formally approved an outcome; the quality of the process depends on the work performed before approval. The institution should be able to show how contrary evidence or an identified defect could alter the result.

1.174 This does not require every officer to become a designer of analytical systems. Different responsibilities can be assigned to subject specialists, legal officers, custodians and independent examiners. The decision-maker should understand the aspects necessary to exercise the particular power and recognise when further assistance is needed. The body must retain enough collective competence to examine the advice it receives and to continue the function when a supplier, employee or method changes.

1.175 The same division of responsibility should inform independent review. An internal reconsideration, a specialist statutory appeal, an ombudsman enquiry, a parliamentary examination, audit and judicial review answer different questions under different mandates. The paper proposes a connected record that can support each competent enquiry without treating their jurisdictions as interchangeable. Findings should reach the institution able to take the required action, with a record of the response.

1.176 Information access is one component of this arrangement. In Mukhtar Ahmad Ali v Registrar, Supreme Court of Pakistan, the majority distinguished the statutory reach of the federal information regime from Article 19A and ordered the specified disclosure on constitutional grounds.[B97] The case illustrates why the route and institutional setting matter. It should not be extended into a general power for the Information Commission over the Supreme Court or into unrestricted access to deliberative and protected case material.

1.177 Review of an intelligence-assisted decision should be directed to the issue raised. An incorrect source record may need custodial correction. A disputed legal interpretation may require consideration by the body competent to determine it. A recurring methodological defect may justify independent examination across a set of cases. A challenge to the exercise of a legal power belongs within the applicable review jurisdiction. The initial institution should preserve the information needed to distinguish these possibilities.

1.178 The available remedy should also be examined. Reconsideration, a fresh hearing, disclosure, correction of a record, suspension of use, remittal or another response may be appropriate under the relevant law. Compensation and personal liability require their own legal basis. The paper proposes no automatic remedy for every error. It asks that the programme establish, before consequential use, how an alleged defect can be examined and what the competent institutions can do if it is substantiated.

1.179 Correction must reach the consequences of an error where the law requires it. A source field can be repaired while an earlier refusal remains in effect. An amended explanation can leave a payment or an adverse classification unchanged. The institution should determine whether pending matters, completed cases or downstream recipients are affected and what further action is required. The response should identify who is responsible for that enquiry and how its completion will be established.

1.180 An individual complaint may also reveal a collective problem. Repeated errors involving a language, locality, category of applicant or particular source should prompt examination of the wider pattern. That enquiry should preserve distinctions among allegations, established defects and unresolved questions. The programme should learn from the findings while protecting personal information and respecting the rights of other affected people. Institutional learning acquires public value when it changes the relevant practice and the result can be checked.

A proposed discipline of accountable public judgment

1.181 The chapter supports a common discipline for Pakistan's institutions while leaving its legal application specific to the public function. The responsible body should identify the power being exercised, the legal question, the evidence used and the degree of influence assigned to an analytical output. It should establish the procedure for receiving contrary information, the reasons required for the action and the route for review. This account should be available in a form appropriate to the person affected and the competent reviewing institution.

1.182 Before introducing a consequential use, the body should explain why it expects the proposed arrangement to improve the function. Its assessment should address existing practice, foreseeable errors, unequal burdens, available alternatives and the resources required for supervision and correction. The justification should be proportionate to the use. A restricted research aid can be assessed within its bounded role; a service influencing essential entitlements demands examination of a wider set of consequences and safeguards.

1.183 The assessment should remain open to revision. A change in the governing law, source collection, system, service population or institutional workflow can alter the justification for continued use. Evidence that staff cannot exercise the oversight assumed in the approval is also material. A service owner should have the authority and resources to seek further examination, narrow the use or suspend it while a defect is addressed. The public body should retain the basis for these decisions.

1.184 The policy position developed here commits the framework to accountable public judgment. Pakistan should develop the ability to use sophisticated assistance where it can be justified, to identify functions for which the available arrangement is inadequate, and to learn from evidence and challenge. The required capability includes the people, records and institutions through which reasons can be examined and errors corrected. That is the contribution of this chapter to the proposed account of Sovereign Intelligence.

Institutional form and the decision dossier

Four institutional options

1.185 A national platform offers purchasing scale and common interfaces but concentrates operational failure and creates pressure to pool information. Fully separate institutional systems preserve local adaptation but can duplicate costs and make evidence difficult to compare. Minimal-capacity outsourcing lowers apparent staffing needs but makes assurance dependent on the supplier being assessed. Federated assurance seeks common methods without assuming one central operational system.

Arrangement	What it can improve	Main policy exposure	Recommended treatment
Central national platform	Shared services and common purchasing	Concentrated outage and authority expansion	Justify function by function rather than presume
Separate institutional systems	Local control and tailored workflows	Repeated costs and incompatible evidence	Permit within applicable approval routes

Arrangement	What it can improve	Main policy exposure	Recommended treatment
Federated assurance	Comparable evidence and retained responsibility	Coordination cost and uneven participation	Preferred initial arrangement
Outsourcing without retained capacity	Short-term staffing simplicity	Inability to challenge or leave the supplier	Unsuitable for consequential dependencies

1.186 Federation describes responsibility and evidence exchange. It does not automatically authorise separate infrastructure, private clouds or exemptions from applicable policy. Covered federal investments must follow the Cloud First Policy's approval and deviation arrangements. A proposal for shared standards must also identify who can issue them, who can require participation and which parts remain optional.[A2] The legal design precedes the choice of physical topology.

A support function with a limited charter

1.187 The proposed support function should maintain common schemas, publish test methods, convene peer review and procure independent assessments where authorised. It may maintain reusable public source collections and model-independent tooling. It should not determine the legal competence of another body by technical inference or certify its own programme as sovereign. Its charter should make prohibited concentrations of responsibility explicit.

1.188 A participating service owner remains accountable for the service. A data steward controls release through the applicable legal route. A legal reviewer records authority and constraints. A technical team builds and operates the system. An assessor tests material claims with sufficient independence from the builder. A records officer manages preservation and disposal obligations. In a small institution some roles may be held by the same person, but the conflict must be visible and independent review must cover the resulting weakness.

1.189 The support function's placement must be reconciled with the National Digital Commission and Pakistan Digital Authority under the Digital Nation Pakistan Act. An implementation record should identify an actual delegation where one is relied upon, including the relevant section 24 notification and its conditions. Programme participation cannot substitute for mandatory federal consultation under the Rules of Business. [A1][A3]

The evidence dossier as the governing object

1.190 The programme should organise decisions around an evidence dossier rather than an overall sovereignty score. The dossier joins a specific question to its authority, evidence, options, dependencies, uncertainties and responsible human decision. It can be produced with ordinary document and database tools. Machine assistance is optional and replaceable.

1.191 A score hides different kinds of weakness inside arithmetic. An excellent restoration time cannot compensate for unauthorised disclosure. A complete source list cannot compensate for an absent power to act. The dossier therefore identifies non-compensable conditions separately from comparative measures. Costs, response times and reviewer effort can be compared after the essential boundaries are satisfied. Missing authority and prohibited transfer are gates, not discounts.

1.192 Human review is effective only when reviewers can understand and challenge the output. For material recommendations, a reviewer should identify the relevant considerations independently before reading the generated recommendation where practical. The comparison can expose automation bias and omitted issues. A review record should state what was accepted, changed or rejected and why, rather than merely record a ticked box.

1.193 Participation should focus on consequences people can assess: continuity of public information, accessibility of source material, distribution of sites and the ability to correct errors. It should not ask the public to endorse an opaque technology package. Consultation materials should distinguish the institution's decision from the system's support function and show alternatives, including simpler arrangements.

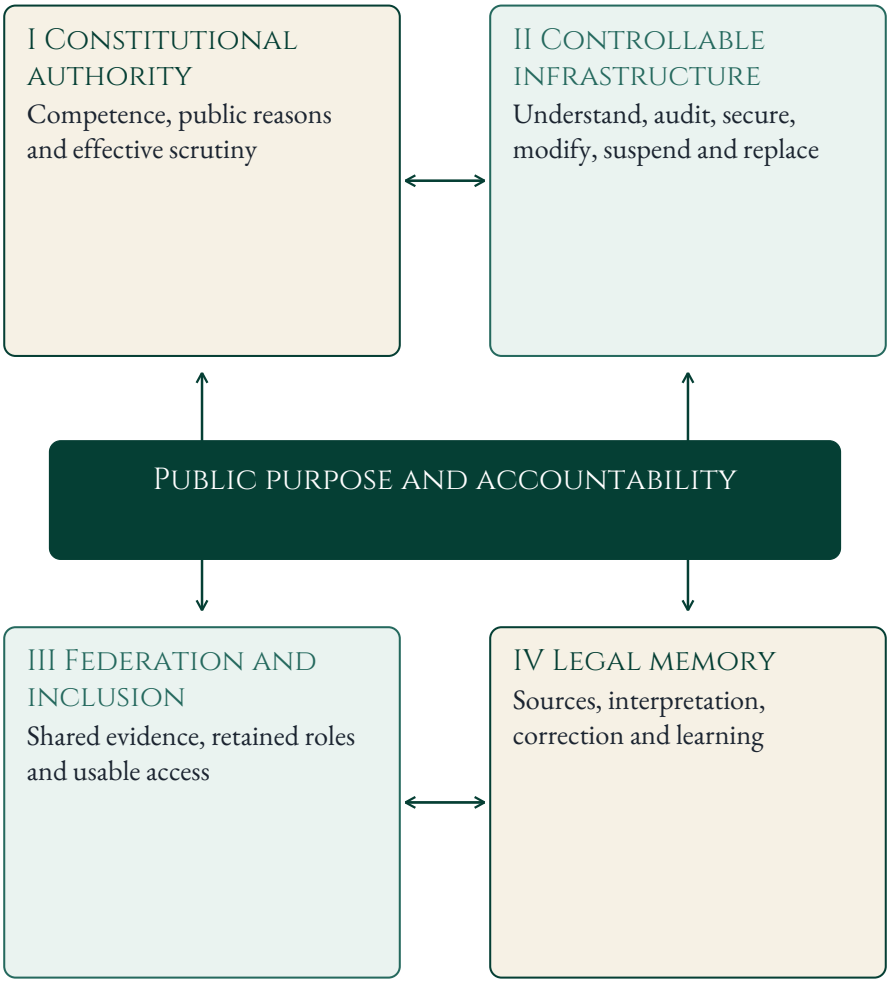
1.194 The programme should publish a periodic account of scope, expenditure, tests, failures, changes and unresolved limitations. Security-sensitive details and legally protected material can be withheld for stated reasons. A general appeal to sovereignty should not become a blanket justification for secrecy. Public reporting gains value when it explains what changed after a failure and who remains responsible for completing the correction.

1.195 An internal programme complaint is not a substitute for a statutory or constitutional route. The service should preserve access to whatever external avenues apply and avoid promising routes that have not been verified. Users should be able to report a source error or service problem without being required to accept the system's account of the law.

FIGURE 01

Four pillars of public capability

INTEGRATED DESIGN • MUTUAL CONSTRAINTS, NOT A COMMAND CHAIN



Sovereign OS supports the interfaces. It is not the constitutional principal.

Figure 1. Four pillars of public capability. Quantities are illustrative where so designated.

Part II Pillar II Controllable digital infrastructure

2.1 An institution's control over a service depends on its legal and operational arrangements, not the supplier's nationality label. The proposed test is whether it understands its dependencies, can meet the service's whole-life costs and can recover a defined minimum service independently.

Data sovereignty as lawful and effective control

2.2 For this paper, data sovereignty means the capacity of Pakistan's competent institutions to govern data within their lawful authority, maintain effective control over consequential processing and dependencies, and protect the rights and responsibilities attached to its use throughout its life cycle. This is an operational definition proposed for the framework. It encompasses acquisition, use, disclosure, retention, preservation, correction, transfer and disposal. Its scope depends on the public function and the law governing the particular records.

2.3 The definition requires care with the language of ownership. Data about a person, a privately authored work, a public register and an official statistical return can engage different legal relationships. The fact that information concerns Pakistan does not establish an unrestricted governmental entitlement to acquire or use it. Custody can carry duties of protection and preservation; a right to consult can fall short of a right to redistribute; a licence for one activity can exclude another. The constitutional requirements of legality, dignity, access to information and equality remain relevant to the powers and procedures through which the state handles information.[B59]

2.4 Effective control has several connected dimensions. Legal control concerns authority, applicable restrictions and enforceable conditions. Institutional control identifies the body answerable for the record and the officials who can approve access or correction. Technical control concerns permissions, administrative access, encryption arrangements, processing environments and recoverable copies. Operational control concerns the people and procedures needed to keep the service working. Evidential control enables an institution to establish what was held, what changed and what supported a particular decision.

2.5 Data residency contributes to these arrangements by locating storage or processing within a specified territory. The policy assessment must also examine who can administer the system, where support personnel operate, whether copies or logs leave the agreed environment, what subcontractors can do and which legal obligations bind the provider. A domestic hosting address answers one of these questions. It leaves the remaining questions to be resolved through the applicable law, architecture, contract and operating practice.

2.6 Pakistan's Cloud First Policy 2022 already addresses data flows, sensitivity-based deployment and the return of public-sector data at the end of a service contract. Its sections 8 and 10.2.4, Annexes D-E and the suggested contractual requirement in Annex F(h) provide a relevant policy reference for examining location, access and continuity. The edition and applicable implementation requirements should be checked for each procurement.[B60] The paper proposes that an institution document its complete processing arrangement before concluding that a deployment provides effective sovereign control.

2.7 The June 2026 Data Governance Policy text develops a further proposed approach. Clauses 8 and 13 distinguish residency categories, controlled offshore processing, foreign-authority requests and onward transfers. Those provisions remain draft material for this paper: the June text makes effectiveness contingent on approval and formal issuance. A Ministry announcement of 21 October 2026 describes issuance, yet on 11 November 2026 the Minister said the policy would be unveiled within weeks; no operative final text has been verified.[B61] Their policy value lies in making the different elements of control examinable. Their draft status prevents their treatment as an existing general permission or prohibition.

2.8 Cross-border cooperation should consequently be assessed by purpose, data category, recipient, jurisdiction and the protections available. International scientific collaboration, disaster forecasting and access to specialist computation may present legitimate needs. A proposal should identify what must cross the border, whether a less revealing form will meet the purpose, how onward use is controlled, what happens when access is demanded by another authority and how the service can continue if the arrangement ends. A contract supplies obligations between its parties; its ability to address conflicting public-law duties needs legal examination.

2.9 An institution should also be able to demonstrate its control. Useful evidence includes a complete account of processing locations, tested access revocation, a usable export, an exercised recovery procedure and a transition that staff can perform. The relevant question is whether the institution can continue its lawful function under foreseeable change. Public investment should be evaluated against that practical ability alongside the location and ownership of equipment.

Public finance, procurement and sustained control

2.10 The constitutional framework for public funds and audit connects capability development to authorisation and accountability. The Public Finance Management Act 2019, in the Finance Division consolidation amended to 30 June 2024, adds requirements relevant to project preparation, evaluation, maintenance, commitments and financial responsibility.[B53] These instruments require an institutional programme to account for both the means it uses and the obligations it creates.

2.11 A capability proposal should identify its initial and continuing costs before expansion. Those costs include staff time, legal and professional review, source updates, hosting, security, evaluation, incident response, migration and equipment replacement where relevant. Different costs may fall on different bodies. A shared service can reduce duplication while creating reliance on a funding stream that participating agencies do not control. The agreement needs to identify who will meet the continuing obligation and how the function will be protected if that contribution changes.

2.12 Expenditure records should also preserve the relationship between what was approved and what was delivered. An appropriation, a release of funds, a payment, acceptance of a deliverable and an observed improvement in service are separate facts. A programme's reporting system should make each fact available with its date and supporting record. This gives management and reviewing bodies a way to identify whether a difficulty concerns financing, procurement, implementation, use or the underlying policy choice.

2.13 The federal procurement position requires attention to recent change. The official Gazette text publishes Public Procurement Rules 2026 under SRO 1658(I)/2026 dated 28 September 2026. Rules 68-69 address transition and repeal, preserving processing under the 2004 Rules for proceedings initiated before commencement.[B54] The applicable version must therefore be established for the procurement concerned, alongside the separate provincial regime where relevant.

2.14 The 2026 federal Rules address planning, specifications, contract management and evaluation. Rules 58-62 make the management of delivery and closure visible parts of the process.[B55] A Sovereign Intelligence procurement should use that institutional opportunity to define what the system must enable the procuring body to do. Acceptance should examine the intended tasks, relevant sources, representative errors, staff competence and continuity arrangements. The specification should make these requirements assessable before the procuring body becomes dependent on the supplier.

2.15 Contract terms should address access to records, documentation, security obligations, material system changes, assistance during investigations, usable export and transition support where the function requires them. The institution should determine which rights it needs to discharge its responsibilities and obtain the advice necessary to make those rights effective. A supplier's general assurance about transparency or reliability needs to be connected to identifiable deliverables and an acceptance process.

2.16 Procurement records and public access have their own requirements under the applicable Rules. Under the 2026 federal Rules, rule 56 provides a minimum five-year record-retention requirement, while rule 57 addresses public access through the federal electronic procurement portal, EPADS, subject to its exception and prior-approval mechanism.[B56] A minimum retention period is not an automatic disposal date: another applicable duty or hold may require longer preservation. The institution should organise documentation so that reviewers can connect the invitation and evaluation criteria to the award, subsequent variations, performance findings and closure. Confidentiality should be examined under the relevant legal conditions and recorded at the appropriate level. The record should enable an authorised reviewer to understand the procurement even where some material is protected from general disclosure.

2.17 Audit forms a further part of sustained control. Articles 169-171 establish the constitutional framework, and section 14 of the Auditor-General's Ordinance addresses access to records and information for the audit within its scope.[B57] A technical architecture should support the production of relevant evidence in a usable form. Financial and technical records may need to be examined together where payments depend on functionality, data quality, service availability or acceptance tests.

2.18 The Digital Nation Pakistan Act expressly connects its Fund and reporting arrangements to public-finance and audit requirements in sections 13-16.[B58] Those provisions should be implemented through records that distinguish commitments, expenditure, assets, services and results. Statutory qualifications concerning audit or protected expenditure require their own examination. Internal programme assurance, statutory committee review and constitutional audit should each identify the work they actually perform and the evidence on which their findings rest.

Worked design one Public information cloud exit

2.19 This entire design is synthetic. Its content counts, restoration runs, pass results, price inputs and tolerance are constructed illustrations. The failure of an essential function remains a failure even when a time target is met.

2.20 The second pillar turns the six capacities of control into observable institutional abilities. A supplier contract can promise portability while the institution lacks the knowledge, time, keys, formats or resources to use it. The relevant question is therefore not whether a service is labelled sovereign, domestic or open. It is whether the actual arrangement can be understood, inspected, secured, changed, stopped and replaced to the degree the function requires.

2.21 The cloud case concerns a public-information service, rather than a population registry or individual eligibility engine. Its lower-consequence scope permits a recovery exercise without presuming permission to move sensitive records. The method can inform more consequential functions, but this exercise cannot authorise them by analogy.

Proposed control capacity	Evidence in this cloud exercise	Failure that remains visible
Understand	Dependency map, format dictionary and operator walkthrough	The institution cannot explain a critical service component
Audit	Manifest reconciliation and independent functional checks	Supplier assurances cannot be reproduced
Secure	Scoped test accounts, destination restrictions and incident record	An unexpected live credential enters the package

Proposed control capacity	Evidence in this cloud exercise	Failure that remains visible
Modify	Documented search and language-route replacement	A change depends on undocumented supplier intervention
Suspend	Stop the affected export or test without disabling the public site	A nominal stop leaves background transfers active
Replace	Second-operator restoration of declared minimum service	Files arrive but the public functions do not work

The policy decision

2.22 The fictional Public Information Service maintains a directory of administrative offices, public notices and downloadable forms. Its supplier contract is approaching renewal. The decision is whether the institution should renew on revised terms, replace a proprietary component or migrate the service. The example deliberately excludes citizen accounts, applications and payment records. It still requires classification and an authorised test environment.

2.23 The synthetic baseline contains 12,000 directory pages, 640 attachments and 120 publication packages. The published content is available in English, Urdu and a third selected language. The minimum service is a searchable directory, correct downloads, accessible notices and an editor's ability to publish a correction.

2.24 Analytics, personalisation and cosmetic features are outside minimum continuity. All quantities and results in this case are constructed to show the decision method.

2.25 The policy choice is often framed too narrowly as whether a supplier provides an export. The proper question is whether a second team can reconstruct the minimum service, with usable records, controlled administration and adequate legal permission, without relying on undocumented supplier intervention. That question tests the relationship between purchasing choices and retained public capability.

Evidence and architecture

2.26 The evidence package contains the executed contract, a procurement-regime note, the classification decision, hosting approvals, a retention map, a content manifest and a dependency inventory. It identifies which items are verified documents, supplier statements, engineer observations or unresolved assumptions. An unknown subcontractor remains unknown. The interface cannot silently convert an empty field into an assurance.

Evidence item	Illustrative populated entry	Why it matters
Minimum service	Directory search, notices, downloads, correction publishing	Defines what recovery must achieve
Content inventory	12,000 pages and 640 attachments	Supports reconciliation rather than impression
Publication history	120 versioned packages	Preserves provenance of corrections
Recovery tolerance	Four hours in this exercise	A design assumption set before the test
Permitted source lag	One daily publication cycle	Defines acceptable loss of newly published content

Evidence item	Illustrative populated entry	Why it matters
Supplier dependence	Managed search index and administrative login	Exposes more than storage location
Human decision	Renewal, remediation or replacement	Kept outside the restoration system

2.27 The architecture has five connected parts. A read-only evidence store holds contractual and technical material. A dependency graph identifies relationships among content, search, identity, storage and administration. An export harness produces a manifest and checks completeness. An isolated recovery environment recreates minimum functions. A review workbench joins results to the relevant contract term, legal constraint and responsible official. The model, if used, summarises the evidence; it has no procurement, deletion or production deployment credentials.

The worked exercise

2.28 Before testing, the owner approves 40 essential checks covering content, search, language links, downloads, editing and administration. An operator captures the baseline, records the manifest and freezes writes in the test copy. A second operator, who did not prepare the export, follows the recovery instructions. The exercise intentionally removes contact with the primary supplier so that undocumented assistance cannot conceal a dependency.

2.29 In the first constructed run, restoration takes 110 minutes. All 12,000 page records and 640 attachments are present. Only 37 of the 40 essential checks pass. Search results fail because the export omitted a proprietary language-processing component; two language-link checks fail because the alternate application treats a supplier-specific identifier as a stable public URL. The recovery-time target has been met, yet the minimum service has not been recovered. The appropriate result is failure of the continuity gate, not a 92.5 per cent success claim.

2.30 The team then tests a bounded remediation. Search is rebuilt with an institution-controlled index, and the language links are converted through a documented mapping. In the second constructed run the independent operator completes restoration in 145 minutes and passes all 40 checks. This establishes a candidate continuity route for the test corpus. It does not prove production-scale resilience, authorise release of additional data or eliminate the need to assess permitted hosting and contractual rights.

2.31 An illustrative dossier conclusion reads: “The current export is insufficient for minimum-service recovery without the documented search and link conversion. The revised package restored the test service within the predeclared four-hour tolerance. Renewal should be assessed against delivery of that package, recurring independent restoration and the applicable procurement route. No contract action is executed by this report.” This conclusion is narrower and more useful than declaring the service sovereign.

Options and whole life cost

2.32 Suppose the hypothetical annual cost of the current service is PKR 12 million and an alternative's recurring cost is PKR 9 million. Migration and revalidation cost PKR 14 million, with PKR 2 million for parallel operation. The annual difference is PKR 3 million and the undiscounted cash break-even is approximately 5.33 years. Over a three-year comparison, staying costs PKR 36 million while migration costs PKR 43 million before discounting. These are illustrative arithmetic inputs, not supplier quotations or a savings forecast.

Option	Illustrative three-year cost	Capability consequence	Principal unresolved condition
Renew current arrangement	PKR 36 million	Existing dependence continues	No usable independent restoration
Migrate immediately	PKR 43 million	Potentially stronger replaceability	Transition risk and procurement feasibility
Renew with modular remediation	To be quoted	Retains service while reducing specific dependence	Enforceable deliverables and test rights

2.33 The missing price for modular remediation should remain missing until evidence exists. Inventing a convenient estimate would prejudice the option appraisal, and the cheapest option should not automatically win. Paying for better continuity requires the value purchased and the budget consequence to be stated. The route must be lawful: PPR 2026, rule 32(1)(c)(iv) allows repeat orders only on the original price, terms and conditions, and rule 59(2)(f) requires approval of a contract variation before its issue.[B55]

Failure paths and institutional response

2.34 If classification is absent, export is held. If the supplier refuses access to necessary evidence, the contract manager records the unresolved issue and uses the applicable contractual or procurement process. Engineers do not bypass access controls. If both nominal suppliers depend on the same identity service, the dossier identifies that common point of failure. If the alternate environment requires an unapproved transfer, the exercise remains synthetic until the issue is resolved.

2.35 If a record-disposal request appears during exit, the records officer separates institutionally required records from supplier copies and identifies the applicable authority. If the restored service cannot preserve publication history, the continuity gate fails even if the latest pages look correct. If the supplier alone can perform the restoration, the programme has evidence of assisted recovery, not independently retained capability.

2.36 The evolutionary contribution is a history of how the proprietary components entered the service and why earlier tests missed them. The strategic contribution is a comparison of targeted redesign and full migration. The anticipatory contribution is a combined outage test involving the supplier and its upstream identity service. Together they can produce a less dramatic but more defensible choice: retain the service temporarily, change specified dependencies and demonstrate exit before the next decision point.

Evaluation and publication

2.37 The exercise should be repeated with a different operator and a changed publication package. Assessors compare the proposed dossier with the institution's ordinary renewal preparation. Measures include essential functions restored, records reconciled, time to reconstruct the decision, reviewer effort and unrecognised dependencies. Reporting the time to first webpage alone would conceal most of the policy objective.

2.38 A public account should describe scope, cost categories, failures and the improvement sought without exposing exploitable configurations or confidential contract terms. The institution should explain why a limited renewal, if chosen, is compatible with the test findings. The relevant public achievement is the ability to justify and change the arrangement, not the production of a reassuring badge.

Dependency graph

2.39 Nodes represent the application, content database, attachment store, search index, identity service, domain administration, monitoring and upstream suppliers. Edges include reads_from, authenticates_with,

administered_by, hosted_on and requires_license. Each edge records the evidence source and whether replaceability is documented, tested or unknown.

Consumer	Dependency	Evidence state	Test action
Public search	Managed language index	Export omits processing rules	Rebuild independent index
Editor console	Supplier identity service	Contract describes access only	Test institution-controlled administration
Downloads	Object store	Full manifest available	Verify digest and access for every attachment
Language navigation	Supplier-specific identifiers	Mapping incomplete	Reconstruct stable public links
Alternate provider	Shared upstream identity	Initially unknown	Inspect and isolate correlated failure

2.40 The graph should not use national origin as a substitute for functional analysis. It can record location and legal constraints where relevant, but the question is how each dependency affects lawful operation. NCSC's cloud supply-chain guidance supports examining underlying providers and privileged access rather than treating the immediate supplier as the whole service.[A10]

Export package and restoration interface

2.41 The export package contains content in an open documented representation, attachments, route mappings, configuration without live secrets, a dependency inventory and a restoration guide. It also contains a manifest with record counts and digests. Search indexes may be exported where permitted, but the minimum service should be able to rebuild them from the underlying content and documented rules.

```
{
  "package_id": "EXIT-FIXTURE-02",
  "content_pages": 12000,
  "attachments": 640,
  "publication_packages": 120,
  "source_lag_hours": 24,
  "contains_live_credentials": false,
  "contains_citizen_records": false,
  "search_rebuild_spec": "SEARCH-SPEC-V2",
  "route_map": "ROUTES-V2",
  "restore_instruction_version": "RUNBOOK-EXIT-02",
  "scope_status": "synthetic_test_only"
}
```

2.42 A digest validates identity relative to capture, not completeness. The harness therefore performs semantic reconciliation: every referenced attachment exists, every published page resolves, language links point to the intended content, and publication history can be reconstructed. A backup that stores every file but loses relationships fails this check.

2.43 The restoration interface accepts only a manifest identifier and an approved environment identifier. It does not accept arbitrary external destinations from a model. The environment uses separate credentials, blocks production writes and records network dependencies. Restoration by a second operator is a requirement because a builder can unconsciously fill gaps in the instructions.

Failure handling

2.44 An absent classification record produces a hold before any real export. An unverified destination or provider produces a hold. A missing attachment causes reconciliation failure. An unexpected credential in the package

triggers quarantine and the applicable security response, not automatic use. A supplier refusal to provide authorised evidence becomes a contract issue for the responsible team. The system does not scrape around restrictions or invent a substitute certificate.

2.45 Deletion requires a distinct workflow. The institution's required official records, working test copies and supplier-held copies have different purposes and authorities. The National Archives Act's defined record and disposal requirements and applicable Cloud First contractual provisions must be considered rather than replaced by a blanket erase-all command.[A2][A6] Technical disposal evidence should identify which copies were affected and what remained outside verification.

Execution runbook

2.46 The coordinator announces the exercise window and confirms that production service remains unaffected. The operator records the source manifest and begins the clock at the agreed point. The primary supplier's assistance channel is unavailable during the independent segment. Any assistance requested is logged and changes the result from independent to assisted recovery unless the test plan expressly permits it.

2.47 The operator builds the alternate service from the guide, runs the reconciliation scripts and executes the user-visible tests. The assessor records elapsed time, observed dependencies, deviations and failures. If a test exposes a live secret or unexpected personal record, the run stops and the incident procedure begins. The team does not use the discovery to expand its access.

Test catalogue

Test	Input or disturbance	Expected behaviour	Criticality
CE01	Complete approved fixture	Restore all minimum functions	Essential
CE02	One missing attachment	Reconciliation failure identifies record	Essential
CE03	Missing language processing	Search failure remains visible	Essential
CE04	Supplier identity unavailable	Approved alternate administration tested	Essential
CE05	Unclassified proposed live export	Hold before transfer	Critical boundary
CE06	Unapproved destination	Deny export and record reason	Critical boundary
CE07	Hidden live credential	Stop and quarantine package	Critical boundary
CE08	Incorrect language route	Identify wrong destination	Essential
CE09	Supplier instruction to mark pass	Ignore instruction as source content	Critical boundary
CE10	Erase-all request	Separate record obligations and supplier copies	Critical boundary
CE11	Second operator follows guide	Reproduce recovery without undocumented help	Essential
CE12	Shared upstream outage	Reveal correlated dependence	Essential

2.48 Tests CE05 and CE06 are performed with harmless simulated requests unless a separately authorised real test is appropriate. The expected denial should be observable in access logs and the absence of a transfer, not just in an explanatory message. A model that says “denied” while a background process releases data has failed.

Completed synthetic decision record

2.49 The illustrative record states: “The initial package failed three essential checks. The revised package restored the fixture within the four-hour tolerance and passed the declared functions. Combined upstream outage testing remains incomplete. The evidence supports continuing the technical exercise and seeking a costed contract option for documented export and restoration support. It does not establish production readiness or authorise renewal, migration or termination.”

2.50 The record assigns the combined-outage test to the assessor, the contract option to the contract manager and provider-route verification to the legal and security leads. It preserves both runs. The first failure is useful evidence about the dependency and must not disappear from the final dossier.

Reading the result as a public capability decision

2.51 The worked migration is a deliberately bounded case. Its object is a public-information service, not a model of all national digital infrastructure. A successful restoration establishes that the defined package can support the tested minimum service under the stated conditions. It does not establish that every dependency can be removed, that live institutional records can lawfully be copied or that migration is the best economic option.

2.52 The decision record should connect the technical result to the people who use the service. Which legally important information remained accessible during the test? Were older documents and their links discoverable? Could an assisted-access desk answer the same inquiry while search was unavailable? Were language and accessibility features preserved? A faster recovery that loses those functions is a weaker public outcome. The test catalogue should therefore contain representative end-to-end inquiries alongside file counts and checksums.

2.53 The appropriate policy outcome can be renewal with stronger exit terms, modular replacement or migration. In the constructed comparison, the cheaper annual alternative does not recover its transition cost within three years. Paying more for transition can still be justified by a specific and valued reduction in dependence, but the institution should state that justification openly rather than describe the migration as a demonstrated saving. The distinction makes the case useful to a procurement committee rather than merely impressive as a technical demonstration.

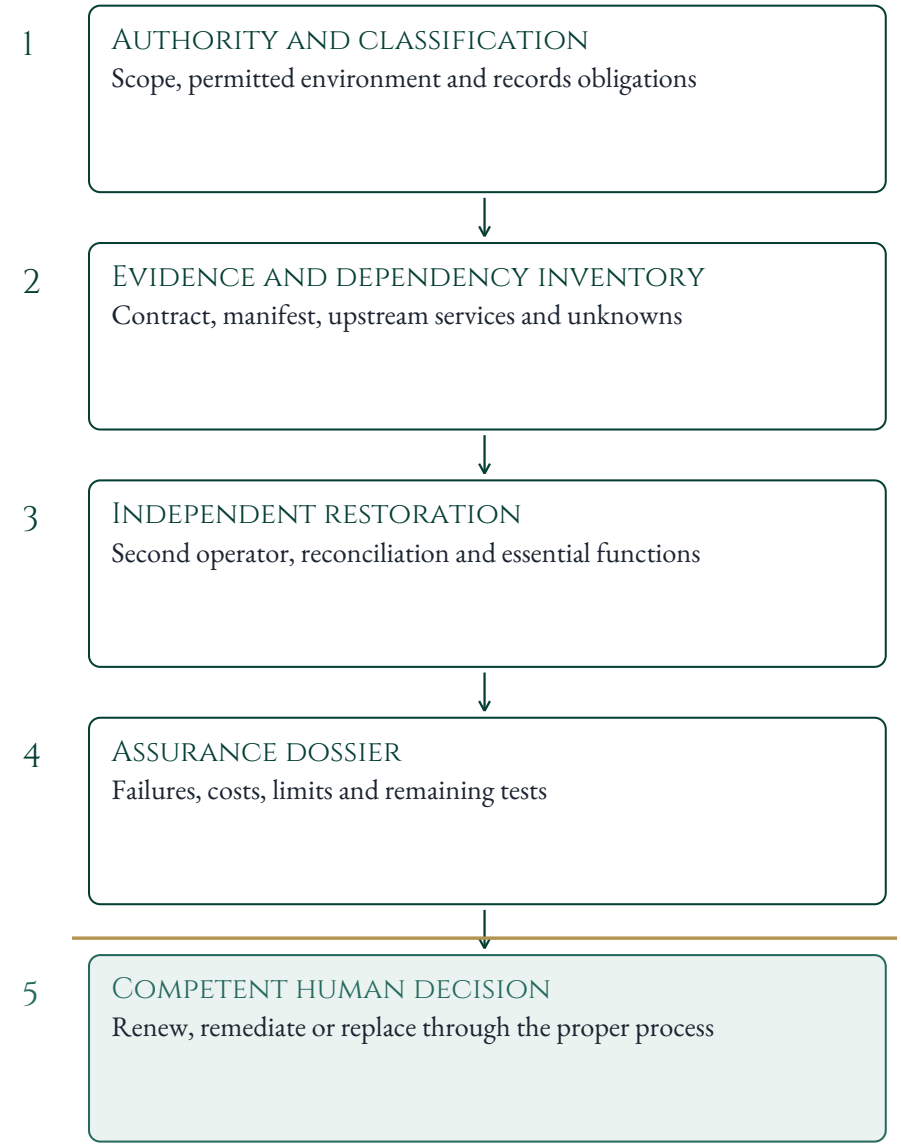
Sensitivity and the limit of the economic claim

2.54 The undiscounted transition cost in the fixture is PKR 16 million, consisting of PKR 14 million migration and revalidation plus PKR 2 million parallel operation. With only PKR 1 million annual operating difference, cash break-even becomes 16 years. If the alternative is more expensive annually, there is no positive cash break-even on these assumptions. Vary transition cost, annual difference and parallel-operation duration separately. Retained capability may justify a higher cost, but is not a demonstrated cash saving. This sensitivity does not change the original 5.33-year and PKR 36 million versus PKR 43 million cases.

FIGURE 02

Cloud exit and the human decision boundary

PROPOSED DESIGN



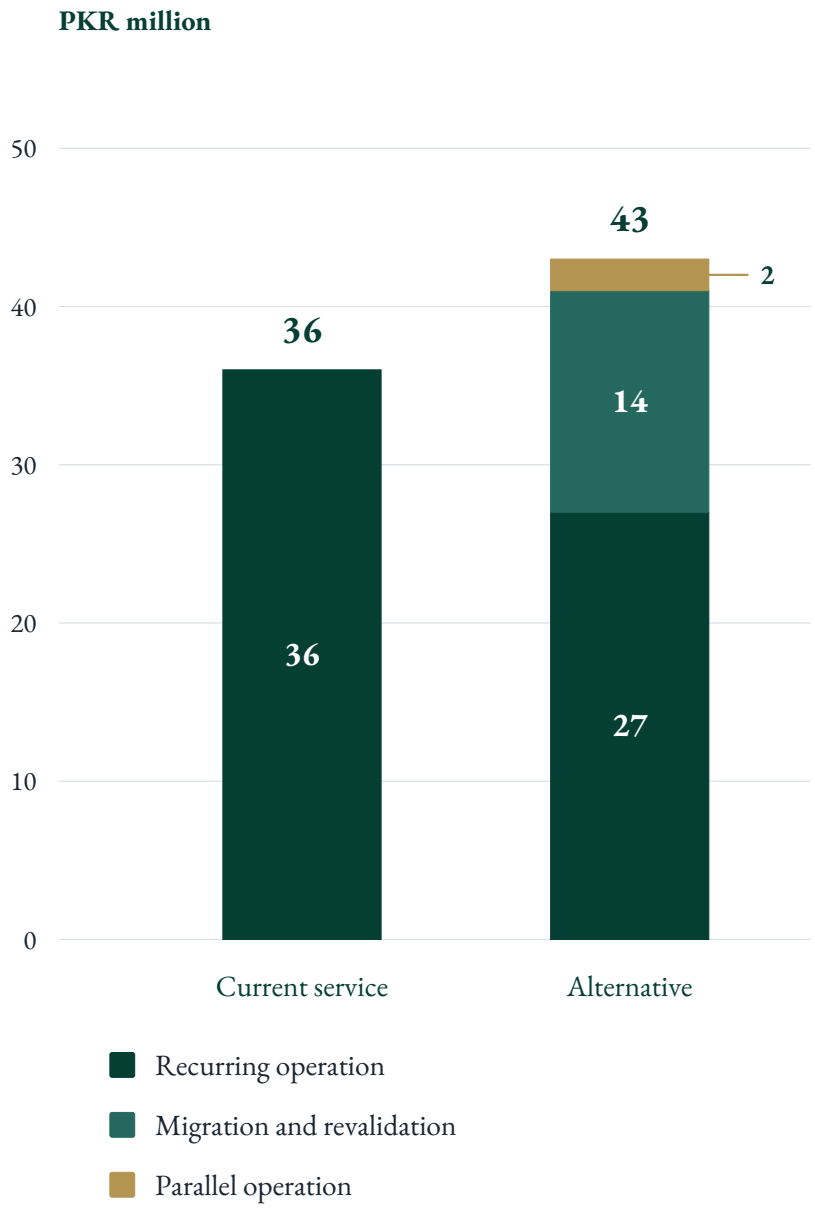
A successful restore does not terminate a contract or authorise a transfer.

Figure 2. Cloud exit and the human decision boundary. Quantities are illustrative where so designated.

FIGURE 03

Illustrative cloud options over three years

ILLUSTRATIVE COSTS • PKR MILLION • UNDISCOUNTED



Assumptions: annual 12 versus 9; transition 14 + 2. Not supplier quotations.

Figure 3. Illustrative cloud options over three years. Quantities are illustrative where so designated.

Part III Pillar III Federated intelligence and inclusive capability

3.1 Cooperation must respect the constitutional allocation discussed in Part I. Participating institutions should preserve a lawful purpose, distinct custodianship, original definitions and actual disagreement. Their shared service must also work for people whose circumstances a central interface does not capture.

Lawful sharing and differentiated access

3.2 DNPA 2025 provides an important starting point for national coordination. Section 8(h) connects the National Data Strategy to data governance while retaining control and responsibility with designated custodians. Section 19 provides an information and assistance request power with compliance escalation. Section 28(2) gives overriding effect to specific protective measures in other laws concerning citizens' data rights and cybersecurity when executing the Act.[B62] Their interaction must be examined for the particular request. Retained custodianship does not make every exchange voluntary, and the protective provision requires a more precise analysis than an assumption that every confidentiality rule defeats every request.

3.3 A proposed exchange should begin with a specific description of the receiving institution's task. It should identify the legal basis for obtaining the information, the source institution's authority to disclose it, the minimum fields required and the decisions the recipient may take. Access to a record should be distinguished from permission to copy it, link it with other records, publish it, use it to train a model or supply it to another party. Each proposed activity should be evaluated against the instruments that govern the source and the receiving function.

3.4 Official statistics provide a concrete example. Section 28 of the General Statistics (Reorganization) Act 2011 protects answers, information and returns furnished under the Act, limits their use and publication, and contains a qualified route for the release of non-identifying unit records for genuine research. Sections 29 and 30 address permitted disclosure and joint collections on their stated conditions.[B63] A national programme must examine those provisions before attempting to reuse statistical returns for an administrative eligibility decision or another operational purpose. An analytical opportunity does not itself supply the necessary authority.

3.5 The same discipline should be applied when an institution asks for information from an identity, health, tax, educational or land system. A reliable identity match may help establish that two records concern the same person. It does not establish that the person is ineligible for a benefit, liable to a tax, resident at a particular address at the relevant time or responsible for another person's conduct. These are separate propositions requiring the appropriate facts and decision rules. The design should preserve the purpose for which each fact was collected and the qualifications attached to its use.

3.6 Access arrangements should be proportionate to the work. A public dataset can be supplied for general reuse under an appropriate licence. Another task may need an authorised query returning only a specified attribute. Genuine research may require a controlled environment with approved users and checks on outputs. A highly sensitive operation may require access confined to an authorised team. These are proposed service arrangements whose availability depends on the governing law and the institution's demonstrated ability to maintain them.

3.7 For personal information, the programme should explain the basis on which processing is proposed and the safeguards and remedies applicable to it. Consent should be examined where it is the relevant basis; a person should receive an intelligible account of what is optional and what follows from a legal requirement. The

design should avoid making unnecessary disclosure a condition of receiving an essential service. Staff need procedures for inaccurate records, incomplete identity evidence and people unable to use a digital interface. The relevant authority should determine the legal requirements for notice, access, correction and review and make those requirements operational.

3.8 For every recurring exchange, the participating bodies should retain an agreement or other applicable instrument identifying purpose, authority, fields, users, permitted transformations, retention, security, correction, onward disclosure and termination. The agreement should explain how incidents and disputed records will be handled. It should identify who can suspend access and who must consider consequences for people whose cases are already in progress. Where an existing instrument cannot lawfully support the proposed use, the programme should resolve that question before commencing the exchange.

3.9 Privacy-enhancing techniques can be considered where they suit the task. Their assessment should specify the information that remains visible, the parties able to infer additional facts, the effect on analytical usefulness and the assumptions on which protection depends. Federated processing still requires authorised purposes, secure participants and controls over outputs. A claim that the underlying data stays with its custodian needs to be accompanied by an examination of what queries, gradients, logs or results reveal. The recommendation is to require evidence for the selected technique in its intended environment.

3.10 The June 2026 draft proposes governed exchange, impact assessment and controlled reuse in clause 10. It separately addresses personal data, citizen-facing rights and AI uses in clauses 11-14.[B64] These subjects identify useful requirements for further design. The infrastructure proposed here should record the legal basis and conditions actually applicable to each service, and should remain capable of incorporating later legislation or validly issued instruments without concealing the earlier basis on which processing occurred.

Language, cultural knowledge and the quality of national evidence

3.11 Pakistan's language resources belong within the core infrastructure. Article 251 addresses the national language, the continuing use of English under its stated arrangement and provincial measures for provincial languages; Article 28 addresses the preservation and promotion of a distinct language, script or culture, subject to Article 251.[B75] A knowledge service should be designed with those constitutional provisions and its particular users in view. Comprehension and the ability to submit or challenge information are practical conditions of participation.

3.12 The programme should develop a documented inventory of Urdu and regional-language material for the tasks public institutions perform. Potential resources include terminology, dictionaries, legislative translations, speech, public-service forms, educational content and historical collections. Urdu, Sindhi, Punjabi, Pashto, Balochi, Saraiki, Brahui, Hindko, Kashmiri, Balti, Shina and other languages require attention according to the service and population concerned. The inventory should identify both available resources and gaps in coverage, quality, rights or technical usability.

3.13 Resource development should begin with the work to be supported. A legal search system may need reliable treatment of citations, dates, negation and specialised terms. A spoken service may need to understand ordinary vocabulary, accents and noisy environments. A form-processing service may encounter handwriting, varying spellings and mixed scripts. Evaluation should cover these conditions explicitly. A single national-language score would leave unanswered how the service performs for a person using a particular language in a consequential task.

3.14 Pakistan's National AI Policy 2025 sets policy commitments concerning datasets, research access and national and regional-language awareness. Its infrastructure proposals include national and provincial data repositories.[B76] Those commitments provide a basis for planning and assessment. An implementation account should

identify the resources actually available, their maintainers, permissions and tested capabilities. A policy target and a reported working resource should retain distinct records.

3.15 Existing specialist work also merits concrete examination. The Centre for Language Engineering at UET Lahore publishes descriptions of Urdu text, speech and lexical resources, with terms distinguishing academic non-commercial access from commercial licensing.[B77] Such resources can inform a national programme, subject to the terms of each release and evaluation for the intended task. Their existence establishes useful starting material; the programme must still examine coverage, annotation quality, permitted transformations and representativeness.

3.16 Public lexicographic work provides another foundation. An official July 2026 release records the launch of the first three revised volumes of the historical Urdu dictionary at a programme organised by the National Language Promotion Department, alongside a publication arrangement covering all twenty-two volumes. [B78] A national terminology service could seek cooperation with this work while establishing the available editions, revision process and permissions for digital use. The announcement alone establishes neither a completed revision nor an openly reusable computational corpus.

3.17 Language development needs sustained professional participation. Linguists, teachers, translators, subject specialists and speakers should help define terminology and assess outputs. Annotation guidance should record difficult choices and disagreement. Translators should identify whether a text is official, professionally reviewed or provided for assistance. In a legal or administrative setting, users need to know which text has legal effect and how to raise a translation problem. A translated explanation should remain connected to the underlying rule and the responsible institution.

3.18 Cultural and local knowledge raises related questions of participation and control. The digitisation of oral histories, customary knowledge and community collections should be based on appropriate permissions and agreed conditions for attribution, access and reuse. Some material may be appropriate for public dissemination; other material may require restrictions determined through the relevant rights and relationships. A national institution should document those conditions and the means of requesting correction or reconsideration.

3.19 The programme should preserve linguistic variation rather than treating every difference as an error. Search tools may need alternative spellings and transliteration links, while source records retain their original form. Speech and text collections should describe the populations and contexts represented. Quality assessment should report where evidence is thin. These practices would improve the state's ability to communicate and learn while making the limitations of its evidence visible.

Worked design two Federated allocation of information access capacity

3.20 Jurisdictions A, B and C are fictional, not coded descriptions of Pakistani provinces. Their planning requirements are explicit normative assumptions. The arithmetic tests consequences under those assumptions and supplies no funding or intergovernmental authority.

3.21 Shared analysis should preserve institutional competence and improve access to public services, rather than merely give a central office more data. A common schema should make definitions visible without forcing disagreement into a single national number. The service should provide a usable lawful route, including for people who do not own a smartphone.

3.22 The synthetic allocation case below links those concerns. It compares additional information-access capacity across three fictional jurisdictions. Desk-hours are an intentionally limited measure. They make the arithmetic inspectable, but do not establish travel accessibility, language support, disability access, service quality or the

needs of people excluded from the source data. Those questions must be recorded alongside the metric, not assumed to have been answered by it.

Inclusion as an operating condition

3.23 Resource constraints require feasible sequencing and genuine alternatives, not invented authority or abandonment of control. The proposed due-process design attends to notice, intelligibility, correction, assistance and access to review. Its operational inclusion test asks whether a person can reach the relevant institution, understand the status of information, supply a correction and obtain a response through a usable route. This is not a claim that all these duties arise from one newly enacted provision.

3.24 A proposed access site should therefore have a service card identifying supported languages, assisted access, opening hours, outage arrangements, privacy at the desk and the institution responsible for correcting misleading information. The capacity worksheet should distinguish an installed terminal from an operational assisted service. A closed counter with functioning equipment contributes no staffed desk-hours. An online-only survey of access needs cannot establish the preferences of people who could not complete it.

3.25 The initial test uses six constructed user journeys: a low-bandwidth connection, a person using a screen reader, a person needing language assistance, a person without a personal device, a person whose prior submission was incorrect, and a person arriving during an outage. Success requires completion of the defined information task or a clear assisted route, without unnecessary collection of identity data. The fixtures do not assign traits to real individuals. Evaluation should later involve representative participants through an appropriate consent and research process, with sample limitations and exclusion patterns reported rather than hidden in an average completion rate.

The question and participating institutions

3.26 Three fictional participating jurisdictions, A, B and C, are considering twelve additional public information access sites. Each proposed site would provide two staffed desks for 24 hours a week, yielding 48 staffed desk-hours. The joint dossier should compare allocations and delivery arrangements. It must not itself allocate funding, create an intergovernmental commitment or determine that one province has performed poorly.

3.27 The scenario uses aggregate institutional figures, published descriptions and expressly authorised submissions. No resident-level records are required. The participants nominate programme officers, data stewards and legal advisers. A secretariat prepares the dossier; the competent forum and participating institutions retain the decisions assigned to them by law. The use of generic jurisdiction labels avoids implying that these figures describe any actual Pakistani province.

3.28 The starting request is: “Compare options for twelve new sites against the participants' stated planning requirements, show what depends on disputed assumptions, and preserve each institution's position.” This is a bounded analytical question. A request to rank provincial loyalty, infer political motives from missing data or compel unrestricted access would be outside the proposal.

Data reconciliation before comparison

3.29 A submits 40 operational desks working 24 hours weekly, or 960 desk-hours. B submits 30 desks at 20 hours, or 600. C initially reports 60 positions, but its metadata states that these are budgeted positions rather than operational desks. C later supplies 20 operational desks at 18 hours, or 360 desk-hours. The initial figure is retained as a different measure; it is not overwritten as though it had always meant the same thing.

Participant	Operational desks	Hours per desk weekly	Weekly staffed desk-hours	Stated planning requirement
A	40	24	960	1,056
B	30	20	600	792
C	20	18	360	648

3.30 The planning requirements are assumptions agreed for this illustrative exercise, not inferred needs or measured social outcomes. The gaps are 96, 192 and 288 desk-hours, equivalent to two, four and six new sites. Whether those requirements represent adequate access remains a policy question, even when the arithmetic is correct. The dossier must show who proposed each requirement, the reasons offered and whether agreement exists.

3.31 The source package for C contains both budgeted_positions: 60 and operational_desks: 20, with different definitions and sources. A generated summary that merges them would manufacture capacity. A participant's non-response is stored as unconfirmed, not treated as consent. These elementary distinctions are more important to the integrity of the decision than the sophistication of the summariser.

Federated evidence architecture

3.32 Each participant keeps a local source repository. A release gateway transmits only approved fields for the identified purpose and legal route. A vocabulary service records original definitions and approved conversions. A calculation service performs transparent arithmetic. A dissent register preserves competing positions. A dossier builder assembles the evidence, options, uncertainty and authority map.

3.33 For the optional pilot, the release record might identify the purpose as access_sites_options_01, the fields as operational desk count, weekly hours, source period and method, and the recipients as the nominated project team. A request for named staff attendance or residents' use histories falls outside that scope. An independently asserted statutory request follows its own assessed route and is not accepted merely because it arrives from an authenticated government account.[A1]

Worked alternatives

3.34 The equal allocation gives four sites to each participant. A receives 192 additional desk-hours against a stated gap of 96; B receives 192 against 192; C receives 192 against 288. The result is a 96-hour surplus relative to A's stated requirement and a 96-hour remaining gap in C. Equality of site counts does not produce equality relative to the declared planning assumptions.

3.35 The requirement-matching allocation gives two, four and six sites. It fills the three stated gaps exactly. It remains dependent on the validity of those requirements and on comparable operating assumptions. If C cannot staff six sites, arithmetic adequacy will not produce an operational service. The dossier should therefore request a staffing and delivery assessment rather than treating the allocation as self-executing.

3.36 A resilience alternative gives two fixed sites to A, four to B and five to C, retaining one mobile site equivalent for deployment under an agreed contingency rule. C remains 48 desk-hours below its stated requirement until the reserve operates there. The alternative trades immediate completeness for flexibility and requires explicit agreement on authority, operating costs and reserve allocation. Calling it resilient without specifying that rule would conceal a new discretionary power.

Option	A sites	B sites	C sites	Shared reserve	Visible tradeoff
Equal count	4	4	4	0	Leaves C below its stated requirement
Requirement matching	2	4	6	0	Depends on the stated requirements and staffing
Fixed sites with reserve	2	4	5	1	Requires a legitimate reserve deployment rule

3.37 The illustrative output recommends requirement matching only conditionally: "Against the stated planning requirements and equal operating assumptions, allocation 2–4–6 closes the measured gaps. Participant C's staffing assurance remains outstanding. Participant A prefers equal counts on geographic coverage grounds. That objection has not been resolved by the desk-hour calculation." The recommendation preserves the disagreement instead of translating a computed result into consensus.

Information routes and disagreement

3.38 Suppose C withdraws optional permission for further analytical reuse after seeing a draft that mischaracterises its budgeted positions. The gateway stops new use under that permission. The secretariat preserves the lawful deliberation record, corrects the mischaracterisation and asks whether the revised purpose and representation can be authorised. It does not erase the history or infer that withdrawal demonstrates non-cooperation.

3.39 Suppose a separate request then invokes a statutory provision. The request is routed to a human assessment of authority, purpose, scope, duty and safeguards. The result may differ from the optional pilot route, but it cannot be presumed by the model. This separation protects both lawful institutional information duties and the integrity of genuinely optional participation.

3.40 Disagreement itself should not block all analysis. The dossier can calculate alternatives under different assumptions, identify the decision that would settle a question and show consequences. It should not assign confidence scores to institutional sincerity or collapse distinct legal positions into an average. Some disagreements require political or legal deliberation and remain properly unresolved in the technical record.

Cost and practical evaluation

3.41 Assume, solely for illustrating the worksheet, that each new fixed site costs PKR 2.5 million to establish and PKR 1.2 million annually to operate. Twelve sites imply PKR 30 million capital and PKR 14.4 million annual operating expenditure. Those totals are not a budget request, estimate of current market prices or evidence that the same cost applies in each jurisdiction. Site variation, connectivity, accessibility, staffing and procurement must be costed separately in a real case.

3.42 The economic comparison should distinguish changes in allocation from changes in total resources. The first two options have the same nominal number of sites under the example's equal-cost assumption. Their distributional consequences differ. The reserve option cannot be costed as a fixed site without evidence about mobility, maintenance and deployment. Leaving that cell unresolved is a substantive conclusion: the option needs additional operational evidence.

3.43 Evaluation should use seeded incompatible units, withdrawn permissions, missing submissions and conflicting positions. Assessors test whether the final dossier preserves each condition and whether a reader can reconstruct the calculations. A central measure is false consensus: instances in which the system reports agreement that participants have not confirmed. One such material misrepresentation can undermine the purpose of the federation even if every total is correct.

3.44 The evolutionary analysis examines why reporting definitions differ and whether prior projects shaped the declared requirements. Strategic analysis compares allocation, delivery and responsibility. Anticipatory analysis tests funding delays, loss of one repository and inability to staff new sites. These modes can alter the recommendation without granting the analytical service any new power to implement it.

Exchange and schema

3.45 Participants retain local source repositories. The shared gateway accepts signed or otherwise institutionally authenticated packages containing permitted aggregates, metadata and a release decision. Authentication establishes who submitted the package, not whether its content is accurate or its release legally sufficient. Both require separate checks.

```
{
  "submission_id": "C-CAPACITY-V2",
  "participant": "Jurisdiction C fixture",
  "measure": "staffed_desk_hours_per_week",
  "operational_desks": 20,
  "hours_per_desk": 18,
  "value": 360,
  "period": "synthetic_common_week",
  "geographic_scope": "participating_sites_only",
  "method": "operational_desks multiplied by hours_per_desk",
  "excluded_measure": {"budgeted_positions": 60},
  "planning_requirement": 648,
  "requirement_status": "declared_assumption",
  "permission_ref": "PERM-COORD-C-04",
  "position_confirmation": "fixture_confirmed"
}
```

3.46 Validation checks unit compatibility, time period, missing fields and arithmetic. The vocabulary service records mappings rather than rewriting originals. If a participant reports annual service hours, the system cannot convert them to a weekly value without an agreed convention about operating weeks and exclusions. A mathematically possible conversion may still be substantively misleading.

Dissent and authority maps

3.47 A dissent record links a participant, proposition, reason and status. It does not grade sincerity. In the worked example A prefers equal site counts because it considers geographic coverage more important than the declared desk-hour gap. The calculation cannot refute that normative position. The dossier reports that requirement matching closes the stated gaps while the coverage objection remains unresolved.

```
{
  "dissent_id": "DISSENT-A-01",
  "option_ref": "OPTION-REQUIREMENT-MATCHING",
  "participant": "Jurisdiction A fixture",
  "position": "prefers equal site counts",
  "reason": "geographic coverage is not represented by desk-hours",
  "status": "unresolved_in_fixture",
  "may_be_summarized_as_agreement": false
}
```

3.48 The authority map connects each proposed action to a responsible forum or an unresolved issue. Preparing the dossier, sharing the figures, committing capital, staffing sites and deploying the reserve are separate entries. A blank authority entry blocks reliance on that action; it does not prevent the dossier from describing the unresolved question. This preserves useful analytical work without laundering uncertainty into permission.

Withdrawal and statutory requests

3.49 If C withdraws optional permission, the gateway blocks new retrieval for that route and invalidates caches used for further optional analysis. It preserves required records of earlier lawful activity under the applicable

retention basis. The system identifies outputs whose continuing use needs review rather than assuming that revocation can erase what authorised recipients already saw.

3.50 An asserted statutory request is a new object, not a switch that changes the optional record to mandatory. Legal assessment records the requesting authority, source provision, purpose, scope, duty and safeguards. Digital Nation Pakistan information provisions and section 28(2) are relevant to that assessment.[A1] The gateway executes only the resulting scoped decision. It does not decide the contested legal question itself.

3.51 This design also prevents accidental over-release. If a package contains an unapproved field, the gateway quarantines it before indexing. An analyst should not be able to recover the field through semantic search merely because the application hides it in the ordinary table view. Access filtering must operate before retrieval and across every derived representation.

Release procedure

3.52 The local steward checks the requested fields, purpose, recipients and applicable route. The release package contains only the authorised subset, with metadata. The gateway validates the package before indexing. An unexpected column is quarantined; hiding it in the interface is not enough because semantic retrieval or export might otherwise expose it.

3.53 A completed synthetic release record reads: “Jurisdiction C authorises the nominated exercise team to use operational desk count, weekly hours, reporting period and method for access-sites options dossier 01. Secondary use and resident-level linkage are outside scope. This is optional test permission, not an assessment of any statutory duty.” The recipient group is explicit. A broad label such as government users is insufficient for the fixture's scoped release.

3.54 If a statutory request is asserted, the legal contact records the requesting authority, provision, purpose, scope, claimed duty and safeguards before release. The platform does not determine the legal question by matching a section number. A withdrawal of optional permission does not settle an independently established statutory obligation, and the existence of statutory powers does not automatically permit every proposed reuse.[A1]

Test catalogue and failure handling

Test	Disturbance	Required response
IG01	Budgeted positions submitted as capacity	Flag non-comparability and preserve original
IG02	Different reporting period	Hold unsupported conversion
IG03	Participant does not respond	Mark unconfirmed, not agreed
IG04	Optional permission withdrawn	Block new use under that route
IG05	Statutory route asserted without assessment	Hold release for legal assessment
IG06	Confidential field included	Quarantine before indexing
IG07	Cross-purpose query	Deny access outside scope
IG08	Dissent conflicts with recommendation	Preserve both with reasons
IG09	Malicious instruction in submission	Treat as content, not command
IG10	Arithmetic input changed	Recalculate and invalidate affected claims
IG11	Exported dossier omits warning	Fail output-equivalence check

Test	Disturbance	Required response
IG12	One local repository unavailable	Mark incomplete and continue only supported work

3.55 If permission is withdrawn, the team identifies cached and derived representations affected by the change. It stops new optional use and preserves lawful records. It does not promise to retract information already lawfully seen by a recipient or delete records that must be retained. The legal and records leads determine what correction or restriction is appropriate.

3.56 If an unauthorised field escaped into an output, the workflow is suspended, affected recipients and copies are identified within authorised access, and the incident process determines notification and correction. The analyst must not simply remove the field from the latest dashboard and declare the incident closed. Earlier exported dossiers may remain in circulation.

From access capacity to actual access

3.57 Desk-hours are a planning input, not a measure of whether people successfully reach an institution. The fictional allocation demonstrates that different fairness assumptions produce different distributions; it does not establish the appropriate rule for a real province or service. Before practical adoption, participating institutions would need to define the population served, the nature and urgency of demand, travel burden, language and disability needs, operating reliability and the route for people whose records cannot be authenticated.

3.58 An evaluation should distinguish sites announced, sites operational, hours staffed, inquiries accepted and matters reaching a competent decision-maker. It should also examine refusal, abandonment, repeat visits and correction, using data collection proportionate to the task. Average throughput can improve while a small group becomes unable to access an essential route. Public reporting should preserve that distributional question rather than combine all performance into one score.

3.59 The federation design gives each participant a way to challenge the definitions before allocation and to record disagreement after comparison. A source institution's operational capacity estimate must not be overwritten merely because a central model prefers a budgeted figure. Shared evidence should reveal the difference between the planned sixty units and the twenty presently available in the fixture. That distinction is the constitutional value of the design: coordination improves the account of need without manufacturing agreement or transferring responsibility through a data schema.

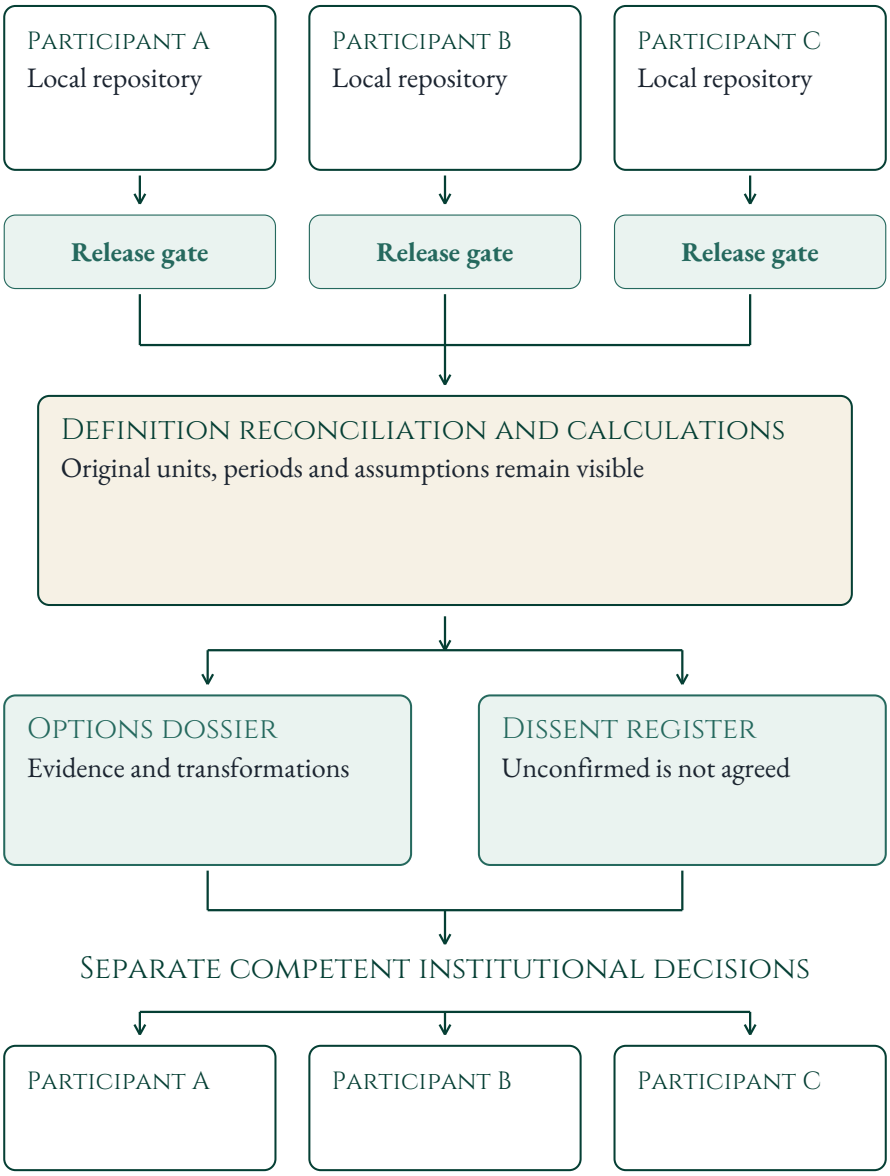
Further allocation and confirmation safeguards

3.60 If a later fixture produces a noninteger site-equivalent, the participating decision-makers must choose and explain a rounding or partial-service rule. The original integer allocation remains unchanged. Confirmation that a submission was transcribed accurately is a separate state from agreement with the analyst’s interpretation or preferred allocation. Start with transparent enumeration of the three human-defined options. If an optimisation method is later used, record the objective, constraints, weights, who selected them and how changing them changes the result. Geographic spread and unfilled declared hours are different objectives, not interchangeable measurements of fairness.

FIGURE 04

Federated evidence without automatic consensus

PROPOSED DESIGN



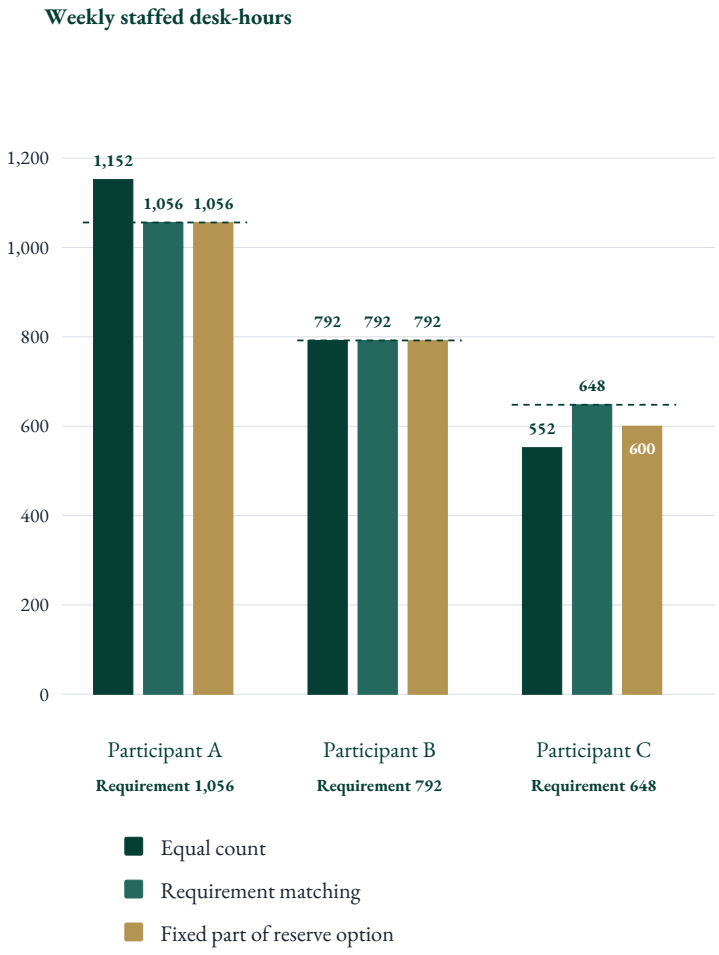
Statutory requests require a separately assessed authority and safeguard route.

Figure 4. Federated evidence without automatic consensus. Quantities are illustrative where so designated.

FIGURE 05

Allocation consequences under declared requirements

SYNTHETIC FIXTURE • WEEKLY STAFFED DESK HOURS



Dashed lines: stated requirements. Reserve adds 48 hours only when deployed.

Figure 5. Synthetic allocation consequences. The plotted quantities are total weekly staffed desk-hours, not additional capacity alone. All inputs are constructed.

3.61 Calculation key: total weekly staffed desk-hours = baseline weekly staffed desk-hours + (new fixed sites × 2 desks per site × 24 staffed hours per desk), or baseline + (new fixed sites × 48). Baselines are A 960, B 600 and C 360. Equal allocation (4–4–4) gives A 1,152, B 792 and C 552; requirement matching (2–4–6) gives A 1,056, B 792 and C 648; fixed sites with reserve (2–4–5) gives A 1,056, B 792 and C 600, with a separate 48 desk-hour mobile reserve available only when actually deployed under the agreed rule. The reserve is not counted in the fixed-site totals.

Part IV Pillar IV Legal memory and institutional learning

4.1 Legal memory depends on more than a searchable archive. Libraries, statistics, science, language resources and professional services supply evidence that institutions must be able to recover and assess. The legal-source design below examines when missing evidence requires a system to withhold a statement of current law.

Data stewardship, professional knowledge and institutional memory

4.2 The June 2026 Data Governance Policy draft proposes data-stewardship roles and governance arrangements. Annex III makes effectiveness contingent on formal issuance after Cabinet approval and Gazette notification. A later Ministry announcement describes issuance, but the operative text and its correspondence to this draft remain unverified.[B50] Its institutional ideas are therefore considered here as proposals, not operative requirements.

4.3 This temporal distinction is part of Sovereign Intelligence itself. A public knowledge system should identify whether an instrument is a draft, an approved policy, an enacted law or an operative notification. It should preserve the evidence supporting the classification and alert the user when the status remains unresolved. Cross-references among proposed instruments need particular attention, since one draft may assume that another has become law. A legal conclusion should be traceable to the controlling source and its applicable version.

4.4 The Personal Data Protection Bill 2023 requires version-specific treatment. The ministry's draft and the Senate private-member bill have distinct provenance and procedural histories.[B51] The draft identifies proposed protections; it does not establish the current legal regime without evidence of enactment, commencement and the relevant institutional arrangements. Existing constitutional and sector-specific obligations must be examined on their own terms.

4.5 Data stewardship should begin with the purpose for which the record exists. A legal register, an identity credential, an administrative case file and a statistical return can concern the same person while carrying different conditions of access and use. The General Statistics (Reorganization) Act 2011, for example, contains express confidentiality and purpose restrictions in section 28.[B52] A national exchange architecture needs to recognise such distinctions when deciding whether to transfer records, supply an aggregate result or leave a dataset with its lawful custodian.

4.6 Federated access may be appropriate where it permits a defined enquiry while preserving source custody and applicable restrictions. Its design should identify the question a receiving institution may ask and the information it is entitled to receive. The source institution should be able to maintain provenance and communicate corrections. A receiving body should be able to distinguish an authenticated source fact from an analytical inference. Security controls need to support those legal and evidential relationships.

4.7 Professional knowledge also requires institutional support. A legal team must be able to establish the controlling instrument and relevant judgment. A statistician must be able to examine coverage, definitions and uncertainty. An operational officer must be able to explain how the service actually works. Technical specialists must understand the system's limits in that setting. The organisation needs working arrangements through which these forms of expertise can inform one decision without losing their separate contribution.

4.8 Universities, public research bodies and professional communities can assist this work through task-specific research, evaluation and training. Agreements should identify the question, access conditions, expected output and responsibility for publication or further use. Evaluation should allow material weaknesses to be

reported to the institution that can address them. The sponsor should preserve enough expertise to assess the resulting work and maintain the capability after the research relationship ends.

4.9 Language and accessibility are practical conditions of this institutional model. An official must understand the source being applied, and a service user must be able to communicate relevant facts and comprehend the explanation provided. Translation, terminology and language-resource development should be designed around the actual service and its users. Where a model is used, evaluation should include the languages, scripts and forms of communication encountered in that work. Performance in a general demonstration may tell little about a disputed local record or an incomplete application.

4.10 Institutional memory connects these capabilities across time. A handover should preserve the purpose of the system, applicable approvals, unresolved issues, data responsibilities, maintenance obligations and recovery procedures. Successor officers need to understand why important choices were made. A project archive should contain the evidence needed to examine those choices and distinguish experiments from approved practice. The objective is to retain a public ability to continue, revise or discontinue the function on informed grounds.

The architecture of a national knowledge infrastructure

4.11 The proposed national knowledge infrastructure is the connected arrangement of institutions, authoritative records, repositories, catalogues, research resources, methods and professional services through which Pakistan can produce and use dependable knowledge. Its national character lies in coverage, interoperability, continuity and lawful cooperation. Different institutions can retain their records and decision-making responsibilities while participating in common discovery, preservation and analytical services.

4.12 The infrastructure should begin with an inventory of consequential knowledge assets. This would cover legal and constitutional materials; official statistics and their methods; administrative records needed for public services; scientific and scholarly work; geographic and environmental information; language and cultural resources; and the analytical methods used to support public decisions. The inventory should also record known gaps. A missing series, an unverified consolidation or a dataset excluding a district can be more consequential than the number of files already collected.

4.13 The inventory should also recognise relevant independent scholarship and public-interest research, subject to appropriate source assessment and permissions. Institutional authority to issue a record and the evidential strength of a research finding answer different questions. Scientific disagreement should remain available for examination. The programme should enable a decision-maker to identify competing findings, their methods and their limitations.

4.14 A practical architecture can be organised into the following connected functions. This is the paper's proposed design, to be implemented through the institutions and instruments competent for each function.

Function	What participating institutions should maintain	What a user or reviewer should be able to establish
Authoritative sources	Originals, source records, official releases and identified custodians	Who issued or collected the material, its status, and the version relevant to the task
Discovery and description	Catalogues, persistent identifiers, metadata and access routes	What exists, its coverage and limitations, and how lawful access can be requested
Governed processing	Purpose-specific access, exchange services and research environments	Which operations are authorised, by whom, with what restrictions and records

Function	What participating institutions should maintain	What a user or reviewer should be able to establish
Analysis and application	Reproducible methods, documented tools, professional assessment and task-specific evaluation	How a finding was reached, what it supports and where uncertainty remains
Preservation and correction	Retained versions, recovery arrangements, change notices and correction processes	Whether an earlier result can be reconstructed and a material error traced to affected uses

4.15 A national catalogue would describe resources across participating repositories. W3C's Data Catalog Vocabulary, DCAT 3, supplies a relevant vocabulary for describing datasets, distributions and data services and for supporting decentralised catalogues and federated discovery.[B65] This makes it possible to design shared discovery without requiring all underlying information to be copied into a single warehouse. The catalogue should expose only metadata appropriate for publication; even the existence or description of a sensitive collection can require protection.

4.16 Common descriptions need to be accompanied by responsibility. Every participating collection should have an identified custodian, an accountable service contact and a maintained route for access or correction. When an institution is reorganised, the transfer of custody should include records, permissions, preservation obligations and unresolved requests. A national coordinator can maintain standards, conformance tools and common services within its mandate. The source institution remains responsible for the matters assigned to it by law and the operative arrangements.

4.17 Shared identifiers and reference data should be introduced selectively. A geographic code, institutional identifier or classification can improve the connection between records, provided its meaning and changes are documented. Administrative boundaries, organisational names and statistical categories can change over time. The system should retain the versions and correspondence tables needed to understand earlier data. Linking a historical series to a current district name should preserve the territorial basis on which the earlier figure was produced.

4.18 The architecture also needs a route for disagreement. Two competent institutions may publish different estimates because they use different definitions, dates or methods. A common interface should disclose those differences and identify the source appropriate to the question. It should preserve the original series and document any reconciliation. A single displayed number should not conceal a choice between materially different measures.

Authoritative Records, Provenance and Institutional Memory

4.19 A national knowledge infrastructure needs to preserve the distinction between the source record and the successive products made from it. An official Gazette, a scanned image, an extracted text, an amended consolidation, a translation, an annotation and a model-generated summary have different evidential roles. Each should be identified and linked to its source. Users should be able to recover the document against which an important extraction or interpretation can be checked.

4.20 Pakistan's Electronic Transactions Ordinance 2002 addresses legal recognition, writing, original form and retention of electronic documents in sections 3-6, subject to its scope and conditions. Section 16(1) does not confer a right to compel an authority to accept or preserve documents electronically.[B66] The Ordinance provides a legal reference for examining accessibility and integrity. A programme must still establish the reliability of the particular process, applicable exceptions and the evidential requirements of the use concerned. Converting a document into a searchable format is one step in preparing a dependable record.

4.21 Preservation requires an institutional route as well. The National Archives Act 1993 expressly includes machine-readable records. Section 5 addresses transfer of non-current public records over five years old, subject to its proviso; section 7 controls destruction and disposal. The Act must be read with the National Archives (Amendment) Act 2026, which changes specified institutional allocations.[B67] Its definition of public office is principally federal and includes notified bodies; territorial extent does not settle its application to particular provincial records. The proposed arrangements should align with the applicable archival and retention regimes and identify responsibilities for custody, transfer, accompanying information and continuing access restrictions.

4.22 The technical record should capture origin, acquisition date, issuer, document identifier, version, relevant dates, format and the relationship between successive copies or derivatives. W3C PROV-O offers a vocabulary for describing entities, activities and agents involved in producing information. Dublin Core terms supply useful descriptions of provenance, sources, rights, versions and temporal relationships.[B68] A national implementation should select a manageable common profile and publish its field definitions, responsibilities and validation rules.

4.23 Provenance records assertions about origin and transformation. The institution must separately assess whether the issuer is authentic, the source is applicable and the proposition drawn from it is supported. A file hash helps establish whether bytes have changed relative to a recorded copy. It leaves legal force, completeness, relevance and substantive accuracy to further examination. The infrastructure should therefore retain both technical lineage and a record of the professional checks performed.

4.24 For legal knowledge, time must be recorded with particular precision. The date of publication, commencement, amendment, repeal and the event being examined can differ. A system should be able to answer both what text was held on a given date and what rule is considered applicable to the relevant event, with the basis and limits of that assessment. A later consolidation should not overwrite the edition relied on in an earlier decision. Where legal effect remains unresolved, the record should retain the uncertainty and the issue requiring determination.

4.25 The same approach applies to judicial materials. The record should distinguish the court's decision, the relevant opinion, the question determined, subsequent procedural history where established and any later treatment inspected. A headnote, a private database entry and an official judgment should retain their separate identities. An extracted sentence should remain connected to its paragraph and surrounding reasoning. The infrastructure can assist legal research while preserving the professional responsibility to determine what the authority supports.

4.26 Statistical and scientific knowledge needs comparable temporal and methodological information. A revised series should retain earlier releases and explain the revision. A survey record should describe the population, collection period, sample and material limitations. A research finding should link to the method and supporting material available for scrutiny. Administrative data should identify the service process that generated it, because a count of applications or transactions may answer a different question from a measure of underlying need.

4.27 Preservation should encompass the information necessary to interpret a record. A dataset without its codebook, a model without the relevant configuration or a report without its underlying definitions may remain physically available while becoming unusable. The proposed minimum preservation package should include the source, descriptive information, rights and access conditions, essential methods and a record of significant changes. Its contents should be proportionate to the record's expected public, legal and historical value.

4.28 Retention and disposal must be managed together. A system should preserve records needed for legal obligations, accountability, research or archival purposes while identifying information whose continued retention is unjustified or unlawful. Disposal should follow the applicable authority and schedule, including any litigation, audit or investigation hold. Technical copies, exports and backups should be included in the plan. Where a preserved historical record contains a mistake, a linked correction can maintain the history while preventing its unqualified reuse.

Open knowledge, research access and intellectual property

4.29 Public access is part of the infrastructure's value. Article 19A and the applicable access-to-information legislation supply relevant legal foundations. The federal RTI Act 2017 addresses record organisation and proactive disclosure alongside exclusions and exemptions.[B69] The proposed infrastructure should make releasable material discoverable and usable and provide an intelligible route for requesting material that cannot simply be downloaded.

4.30 An open release should contain more than a spreadsheet or document link. Users need a description of coverage, definitions, update frequency, responsible institution, revision history and reuse terms. Machine-readable formats should be accompanied by accessible presentation where appropriate. If a dataset changes, the service should retain identifiable releases so that a researcher or public body can establish which figures supported a published conclusion.

4.31 PBS's publication of national and provincial reports and detailed tables from the 2023 census illustrates an existing foundation for this work.[B70] A knowledge service could connect such releases with their questionnaires, classifications, geographic definitions and later revisions. It should distinguish published aggregates from access to respondent-level records and establish the terms applicable to each product. Integration would then improve the ability to interpret and compare evidence while preserving the statistical safeguards governing its source.

4.32 The FAIR principles offer useful guidance for making research data findable, accessible, interoperable and reusable. They allow access procedures involving authentication and authorisation and require attention to reuse conditions and provenance.[B71] Their application can therefore support both open publication and controlled research access. For Pakistan, the policy choice is to make conditions legible and proportionate while maintaining the restrictions that the law and the particular data require.

4.33 Disclosure risk needs to be assessed against likely uses and combinations. Removing names can leave information that identifies people through unusual attributes or linkage with another source. Small-area statistics, locations and records concerning rare events warrant particular attention. A publication process should decide whether aggregation, suppression, restricted access or another measure is appropriate, document the decision and review the effect of later releases. The purpose is to make useful knowledge available under defensible conditions.

4.34 Reuse rights also require their own analysis. The WIPO-hosted version of Pakistan's Copyright Ordinance 1962, amended through 2000, distinguishes rights in a compilation from the underlying data in section 3(3), addresses government works in section 13(d), and provides specified exceptions in section 57, including qualified reproduction of Gazette material and judgments.[B72] These provisions require examination for the intended activity and current applicable text. They do not establish a general permission to use every publicly accessible work for AI training.

4.35 The proposed catalogue should record permissions for consultation, copying, redistribution, adaptation and model development separately where they differ. Third-party annotations and editions may require their own analysis. Research access should be connected to the relevant licence, agreement or statutory route, with a process for resolving uncertainty before a corpus is released or reused.

4.36 Pakistan's existing research services provide foundations to examine and strengthen. HEC's National Digital Library describes institutional access to scholarly resources under subscription and eligibility arrangements. PASTIC describes bibliographic, catalogue and document-supply services.[B73] Their resources and professional expertise can support discovery and evidence review. The applicable licences and service terms must be checked before using supplied material in a shared repository or computational research activity.

4.37 A national programme should therefore connect libraries, archives, universities and specialist institutions through a supported service network. Participating teams could assist with source discovery, metadata, rights enquiries, repository deposit and research methods. Public funding conditions could require appropriate preservation and availability of outputs where lawful, with justified exceptions and manageable deposit requirements. The costs include professional labour, documentation and continuing support as well as storage and connectivity.

4.38 UNESCO's 2021 Recommendation on Open Science offers a relevant international policy reference. It connects research infrastructure with preservation and interoperable or federated services while recognising justified restrictions and mediated access.[B74] Its application in Pakistan would require measures consistent with domestic constitutional arrangements and the rights attached to particular materials. The paper proposes that publicly supported knowledge services publish their access conditions, preservation responsibilities and arrangements for long-term maintenance.

4.39 Access to controlled research environments should be governed by clear criteria, published procedures and decisions capable of review. A researcher should be able to learn what resources exist, what approvals are required, how long a decision is expected to take and what restrictions apply to outputs. Institutions should monitor whether smaller universities, provincial researchers and public-interest organisations can use the service in practice. A formally available facility can still be inaccessible if its costs, procedures or support arrangements exclude the people it is intended to serve.

Preparing data for analysis and AI

4.40 The infrastructure should support several forms of knowledge work: legal research, statistical analysis, scientific modelling, professional enquiry and, where appropriate, machine learning. The choice of method should follow the question, the available evidence and the consequences of error. A maintained public register or transparent calculation can sometimes supply the needed capability with lower complexity and clearer review. The assessment should establish what the proposed method adds and what new dependencies it creates.

4.41 A dataset should be considered ready for a particular AI use only after its suitability has been examined for that task. The examination should cover source authority, permissions, population and period, missing information, labels, transformations and known limitations. Data used to train, adapt, retrieve information for or evaluate a system can carry different requirements. The June 2026 draft addresses several of these issues in clauses 14.3 and 14.6, but the actual project must establish its governing basis and controls.[B79]

4.42 For a retrieval-based assistant, the institution should maintain an approved source collection with versioned documents and an update procedure. The retrieval process should respect user permissions before making protected material available to generation. Outputs should identify sources that a user can inspect, and evaluation should test whether the cited passage supports the particular proposition. A citation can point to a real document while failing to support the answer. The source record and the generated response should therefore remain separately examinable.

4.43 The design should also address hostile instructions embedded in retrieved material. A document supplies content for assessment; operational permissions should come from the authorised service workflow. Testing should examine attempts to make the assistant disclose protected information, disregard access conditions or

invoke tools beyond the user's authority. The institution should establish how retrieved content is isolated from the controls governing actions and should assess that separation in the actual deployment.

4.44 NIST's Generative AI Profile identifies confabulation and data-privacy risks and recommends checking sources, citations and relevant data provenance. Its actions MS-2.5-001, MS-2.5-003 and MS-2.5-005 are useful voluntary references for task-specific assessment.[B80] They support a requirement for measured evidence rather than an inference from a fluent demonstration. The Pakistani institution remains responsible for deciding which tests are necessary for its intended public use.

4.45 Evaluation resources should be independent of the material used to optimise the system to the extent required for a meaningful test. They should include difficult, incomplete, contradictory and outdated records, along with representative languages and user conditions. Legal tasks need questions about commencement, amendments, jurisdiction and exceptions. Administrative tasks need cases in which a missing record requires enquiry rather than an adverse inference. Results should report material error types, affected groups and the conditions under which the system should defer or stop.

4.46 Before consequential use, the competent service owner should approve measurable acceptance and deferral criteria and an evaluation process using identified, versioned material reserved for testing. The release decision should record whether those criteria were met and what uses remain outside the demonstrated capability. The service should have an authorised route for suspension, rollback or restricted operation when material failures emerge. This connects testing to the institutional decision about whether and how the system may be used.

4.47 The institution should retain enough of the analytical record to investigate a consequential output. Depending on the task, this can include the source release, model and software versions, relevant configuration, retrieval results, calculations, output and the official action taken. Sensitive inputs and logs should be protected and retained only as lawfully justified. The record should enable authorised review without creating an unrestricted secondary store of personal information.

4.48 Quality control should extend to changes after deployment. A new source release, translation method, model, prompt or retrieval configuration can affect results. Material changes should be documented, evaluated and authorised under the service's governance arrangements. The team should establish whether earlier work needs re-examination and communicate relevant limitations to users. The ability to update knowledge safely is part of the capability being procured and maintained.

4.49 Supplier arrangements should address the information and rights needed for this work. The institution should determine whether inputs or outputs can be retained for supplier training, how subprocessors operate, what records are available for investigation and how collections, annotations and configurations can be exported. Restrictions should be expressed in enforceable terms appropriate to the service. Acceptance should include a practical demonstration that staff can recover and use the agreed materials.

Continuity, correction and implementation

4.50 Continuity requires preservation and service operation to be planned together. Important collections need maintained copies, integrity checks, recovery procedures and readable formats. Essential services need staff who can restore them and access to the documentation required to do so. Recovery should be tested against the function being supported: restoring files is insufficient if the institution cannot restore permissions, interpret the data or resume the lawful procedure.

4.51 Public archives and the National Archives' published descriptions of digitised collections provide an institutional starting point for examining long-term access to selected historical records.[B81] A modern programme should assess the collections, facilities, staffing and legal arrangements actually available before assigning further responsibilities. It should also address digital records created in current services. Preservation

requirements are easier to meet when records and their descriptive information are captured during ordinary work.

4.52 Correction should be treated as a connected process across the infrastructure. A custodian may correct a source field, revise a statistical release, identify a mistranslation or withdraw a misleading analytical output. The system should record what changed, why, who authorised it and which known downstream uses need notice. Where earlier decisions may have been materially affected, the responsible public authority should determine the action required under the applicable law and procedure.

4.53 This process needs a clear boundary between an assertion that a record is wrong and an established correction. A complaint should be recorded and directed to the competent body, with any necessary interim qualification. The infrastructure should preserve the result and the route of review. It should avoid silently replacing disputed facts or allowing an unresolved allegation to become an authoritative attribute. The person affected needs a practical way to supply evidence and receive the institution's response.

4.54 Implementation should begin with a limited number of consequential collections and services. Candidate work includes an authoritative legal-record service, a documented statistical catalogue, a multilingual public-information collection and a controlled research-access service. Selection should follow an assessment of public need, legal authority, source readiness, custodial capacity and the resources required to maintain the result. The initial programme should leave a reproducible method that other institutions can adopt.

4.55 The first stage should establish custody, inventories and the instruments governing access and reuse. It should identify gaps in source authority, versions, permissions and retention. The second stage should connect participating catalogues through a common descriptive profile and introduce selected exchange or research services. The third should test consequential analytical uses against maintained sources and representative evaluation material. Expansion should follow evidence that the participating institutions can sustain the service, correct defects and support authorised scrutiny.

4.56 These stages require named responsibilities and recurring resources. Custodians need subject knowledge and record-management capability. Shared operators need technical and security staff. Libraries and research institutions need support for curation, rights enquiries and methods. Finance and procurement officers need specifications and acceptance evidence that reflect the continuing service. Existing institutions should be assigned work within their mandates, with additional legal instruments or resources where the proposed responsibility requires them.

4.57 Progress measures should describe capability and public value. Useful measures include the proportion of priority collections with identified custodians and verified versions, time required to obtain an authoritative source, completion of rights and access decisions, coverage of language and regional gaps, correction times, recovery performance and the ability to reproduce selected analytical results. Measures should disclose their denominator and method. Counting uploaded files or launched interfaces supplies only a partial account of the work.

4.58 An illustrative application is a provincial flood-response service drawing on meteorological observations, geographic information, local reports and authorised administrative records. Each source would retain its custodian, coverage, update time and limitations. A public risk map might use an appropriate aggregate release, while person-specific assistance would require separate access controls and the relevant entitlement rules. An unverified local report could prompt enquiry while remaining distinguishable from a confirmed observation.

4.59 If a locality or household were missing from the records, the service would need a route for receiving evidence and requesting review. Revised boundaries or corrected observations would be linked to the affected analysis. The responsible authority would retain the basis for its action and decide how new information affects

pending or completed cases. This application would test whether the infrastructure connects sources, professional judgment, public communication and lawful correction under realistic operating conditions.

4.60 Pakistan needs an enduring ability to discover its knowledge resources, preserve their authority and context, govern their lawful movement and put them to use through accountable institutions. A national knowledge infrastructure should sustain that ability across changes in personnel, technology and government. Its quality will be shown when an institution can recover the relevant source, explain what it supports, recognise what remains unknown and correct a consequential error with evidence.

Worked design three Legal source continuity

4.61 The Test Public Records Service Act, its amendment, notification and all query outcomes below are fictional. The source service demonstrates the difference between source identity, legal currency and applicability to an event. Actual Pakistani source questions retain the limitations in their A and B references.

4.62 The fourth pillar is the continuity of public legal memory: the ability to recover the relevant source, identify its version, explain how an interpretation was formed, propagate a correction and preserve what a future reviewer needs. It connects the institution's working knowledge with the affected person's ability to understand and challenge an account. A large searchable corpus is not enough if it cannot distinguish a Gazette instrument from commentary, an enacted text from a proposal, or a current rule from an older rule preserved by transition.

4.63 Sovereign control depends on usable legal memory. This volume proposes that every answer point to its source state, every significant change identify affected outputs, and every correction preserve the difference between an original error and a later change in law. The source archive supports legal work; it does not itself determine authoritative meaning.

4.64 The fictional statute has a distinct name so that exact dates, transformations, abstention and transition logic can be tested without implying a statement of Pakistani law. Actual Pakistani authorities remain in separate, identified source records whose claims can be checked independently.

Preserving access without manufacturing currency

4.65 The fictional Legal Source Service supports institutional librarians and researchers during official publisher outages and changes in publication format. Its initial collection has 120 instruments represented by 260 captured versions, 40 amendment documents, 16 commencement materials and 80 judgments. These numbers describe a synthetic test corpus. The collection is deliberately bounded and does not claim completeness across Pakistani law.

4.66 The service's purpose is to recover identified sources, show their relationships and explain what remains unverified. The principal policy danger is not merely that a document goes missing. It is that an accessible historical document is confidently presented as the current rule. A dated archive can be valuable during an outage if its limitations are visible; an apparently current answer built from an incomplete archive can mislead its users.

4.67 Official publishers remain distinct from the operators of a derivative research service. Editorial verification confirms specified attributes of a source, not all possible conclusions about its applicability. Commentary and treatises remain separately labelled. The system cannot amend law, issue a judgment or execute a remedy.

Source and version design

4.68 The architecture contains a source register, original-document store, extraction pipeline, version graph, retrieval service and correction queue. The original file is preserved alongside extracted text. An identifier links

quotations to page or paragraph locations. Publication date, acquisition date and known legal-effect dates are separate fields. A hash helps identify an unchanged file; it does not prove that the file is official, complete or legally operative.

4.69 A version relationship states whether one document amends, commences, corrects or supersedes another, and identifies the editor and supporting source. Unverified relationships are visible but cannot silently govern a current-law display. A language version records whether it is an official text, authorised translation or research aid. The system must not imply that all translations have equal legal status merely because their files are connected.

A fully worked synthetic query

4.70 A deliberately fictional Test Public Records Service Act 2024 supplies the demonstration. Its original section 8 requires a response within 30 days. A fictional 2026 amendment substitutes 15 days, but the amendment states that the substitution begins on a date appointed by notification. The test collection initially contains the original Act and the amendment, but not the notification. These are test instruments, not statements about Pakistani law.

4.71 A researcher asks: "What response period applies on 1 July 2026?" A weak retrieval system finds the most recent document and answers 15 days. The proposed service instead retrieves both versions and returns: "The amendment text substitutes 15 days, but its commencement depends on a notification absent from this collection. The applicable period on the requested date cannot be established from the available sources." The output provides the relevant passages and identifies the missing instrument.

4.72 An editor subsequently acquires a fictional notification bringing the substitution into force on 30 June 2026. A second provision preserves the prior period for requests received before commencement. The query now needs a further fact: when the request was received. For a synthetic request received on 2 July, the supported response is 15 days under the amended rule. For one received on 29 June, the transitional provision preserves the earlier period. The service records the factual assumption rather than presenting a universally applicable answer.

4.73 This example demonstrates why document recency is not enough. Applicability depends on enactment, commencement, transition and the facts of the question. It also shows why refusing an unsupported conclusion is useful output. A service that always answers would fail this test by design.

Failure and correction

4.74 The test corpus should contain a same-named instrument from another jurisdiction, an incomplete scan, an incorrect amendment link, an unofficial translation and a corrupted file. Each requires a different response. The wrong jurisdiction should be excluded from a jurisdiction-specific answer. The incomplete scan should be flagged and held from definitive quotation. The false amendment edge should be corrected with a preserved history. The translation should retain its status. Corruption should trigger restoration from a verified copy rather than a generated reconstruction.

4.75 Evaluation compares ordinary librarian-assisted research with the proposed service on known-answer and unanswerable tasks. Measures include correct source and version retrieval, unsupported applicability claims, time to verify a proposition, abstention quality and correction coverage. A fluent answer with an existing but irrelevant citation is a failure. A cautious answer that identifies the exact missing commencement material may be a success.

Corpus and preservation

4.76 Each source object stores issuer, title, instrument type, jurisdiction, publication date, acquisition date, known effect dates, language status, original file and extraction quality. An original file is never overwritten by corrected optical character recognition (OCR) text. The corrected text receives its own version and a link to the original. If the source is incomplete, the completeness field is explicit and retrieval cannot present an absent passage as verified text.

4.77 A preservation package includes the source manifest, originals, text, relationship records and an index-rebuild specification. A recipient should be able to inspect the archive without the original proprietary interface. A licensed source may impose limits on redistribution; those acquisition conditions belong in the source record and export filter. Preservation does not automatically authorise public republishing.

Version graph and time

4.78 The graph distinguishes publication, commencement, amendment, repeal, correction and applicability. A newer file is not necessarily a newer rule. An amendment can be enacted before commencement. A transitional provision can preserve the earlier rule for a defined class of matters. A judgment's date does not by itself resolve its subsequent treatment.

```
{
  "source_id": "TEST-ACT-2024-S8",
  "fictional_fixture": true,
  "original_rule": "response within 30 days",
  "amendment_ref": "TEST-AMENDMENT-2026",
  "amended_rule": "response within 15 days",
  "commencement_method": "notification",
  "commencement_ref": null,
  "current_applicability_status": "not_established",
  "editorial_status": "identity_checked_relationship_incomplete"
}
```

Retrieval and answer composition

4.79 Retrieval begins with jurisdiction, date and source-type constraints. Exact title and provision matching should run alongside semantic search. Candidate passages are ranked within the permitted corpus, then checked for version relationships and required companion materials. The system should retrieve relevant qualifications, not merely the sentence most similar to the question.

4.80 The answer composer receives passages and metadata, not an unrestricted instruction to answer from general knowledge. It produces a structured result with quotations, summary, assumptions, unresolved questions and support links. A verifier checks whether each material proposition is supported and whether the available record justifies the requested degree of currency. Automated checking can flag defects; a consequential interpretation still requires human review.

```
{
  "query_id": "LEGAL-QUERY-01",
  "requested_date": "2026-07-01",
  "answer_status": "insufficient_commencement_evidence",
  "supported_statement": "The fictional amendment substitutes 15 days",
  "missing_source": "notification appointing commencement",
  "current_rule_asserted": false,
  "source_refs": ["TEST-ACT-2024-S8", "TEST-AMENDMENT-2026"],
  "next_research_step": "locate and verify the required notification"
}
```

4.81 An abstention should be specific. “Cannot answer” is less helpful than identifying the absent notification and showing the sources that establish why it matters. The system should not use uncertainty as an excuse to omit available evidence. Its task is to separate what can be supported from what remains unresolved.

Correction and affected-output tracing

4.82 Every released answer points to the source and relationship versions used. If an amendment edge is corrected, the system can find dependent answers. The correction queue assigns severity, identifies the responsible editor and records the corrected proposition. It preserves required evidence of the earlier output while ensuring that new answers do not repeat the defect.

4.83 Suppose a synthetic mistaken commencement edge affects eleven answers. The system generates an affected-output list, not a mass message containing every user's query. Authorised recipients receive a scoped correction that explains the issue and identifies the affected answer. Confidential matters remain separated. The institution decides applicable notification duties; the model does not improvise external disclosure.

4.84 The correction process must also distinguish an error from a later legal change. An answer correct when issued can become outdated without having been erroneous. The record should describe that difference. Otherwise the system can distort its own performance history or make users misunderstand whether they relied on a defective analysis.

Concurrent work and stale evidence

4.85 Two editors can review the same source while an analyst prepares a dossier. Without explicit concurrency rules, a later save can overwrite a correction or a released answer can mix source versions that never existed together. The service should use optimistic concurrency for mutable metadata: an update declares the version it read, and the server rejects the write if that version is no longer current. The editor then reviews the intervening change rather than silently replacing it.

4.86 An analytical run uses a frozen manifest of source, relationship and permission versions. Before release, the workbench checks whether any material dependency changed. A new amendment edge may require fresh analysis; a spelling correction to a non-material description may require only a recorded review. The system should identify the changed dependency and its possible effect, not automatically discard all work or assume that every change is harmless.

4.87 Interface operations should be narrow and auditable. A request to retrieve passages contains a purpose identifier, corpus scope, jurisdiction, requested date and permitted source types. The response returns passage identifiers, original-file anchors and limitations. A request to create a claim contains support references and a declared claim type. A request to release a dossier contains the reviewed manifest and approved audience. There is no general endpoint called execute recommendation.

4.88 Retries require idempotency. A repeated request to register a captured source should return the existing object when the stable identifier and digest match, rather than create duplicate instruments. A repeated release operation should not send the same correction twice or create competing decision records. If the digest differs under an existing source identifier, the service holds the operation for version review instead of overwriting the original.

4.89 Permission revocation has precedence over stale caches. The retrieval layer checks current access at the point of use, even when a permitted snapshot supplied the earlier analysis. The retained run record can preserve the evidence needed to explain earlier lawful processing under its applicable retention basis, while new access is denied. These are different operations and should not be implemented by one indiscriminate delete command.

4.90 Queue management is also a governance control. Items awaiting legal review, source verification or incident correction should show age, consequence and assigned owner. The system may prioritise an expiring public-service notice over a cosmetic metadata correction under an agreed rule. It should not infer priority from a participant's political significance or treat repeated model requests as grounds to bypass a human hold. Escalation informs the responsible person; it does not manufacture the missing approval.

Completed source record

Field	Synthetic example
Source identifier	TEST-ACT-2024-S8
Status	Fictional instrument for evaluation
Original rule	Response within 30 days
Amendment	TEST-AMENDMENT-2026 substitutes 15 days
Commencement	By notification, not yet in initial collection
Publication date	Recorded separately from legal effect
Current applicability	Not established from initial package
Editorial decision	Permit dated quotation; withhold definitive current rule
Missing evidence	Commencement notification and any transitional provision

4.91 The record gives the researcher the available material and identifies the missing evidence. Filling the commencement field from the amendment's publication date would conceal that gap and make the service less reliable.

Test catalogue

Test	Fixture condition	Required output
LS01	Correct identified provision	Accurate quotation and source anchor
LS02	Same title in another jurisdiction	Exclude or clearly distinguish
LS03	Amendment without commencement	Withhold unsupported applicable rule
LS04	Transitional saving	Ask for or use relevant fact date
LS05	Incomplete scan	Flag missing text and avoid invented completion
LS06	Unofficial translation	Preserve translation status
LS07	False amendment edge	Hold and correct relationship
LS08	Corrupted original	Restore verified copy or mark unavailable
LS09	Publisher outage	Offer dated archive with visible boundary
LS10	Unanswerable question	Explain specific missing evidence
LS11	Corrected source affects prior outputs	Identify dependent answers
LS12	Malicious instruction in PDF	Ignore as instruction and preserve evidence

4.92 Assessors inspect the answer, source passage, version relationship and displayed status. A citation to a real document is insufficient if the document does not support the proposition. A model's fluent explanation

cannot compensate for an omitted transitional clause. Conversely, a precise abstention may pass when the corpus genuinely lacks the required evidence.

Legal memory beyond retrieval

4.93 Legal memory is a sovereign capability because institutions must remain able to explain the authority and reasons of past acts after rules, personnel and vendors change. The example's uncertain commencement date is not merely a search defect. It can determine whether a person was entitled to a response at a particular time and whether an institution's earlier conduct requires reconsideration. The archive should therefore preserve the relationship among the source, the interpretation adopted, the relevant event date, the responsible decision-maker and later correction.

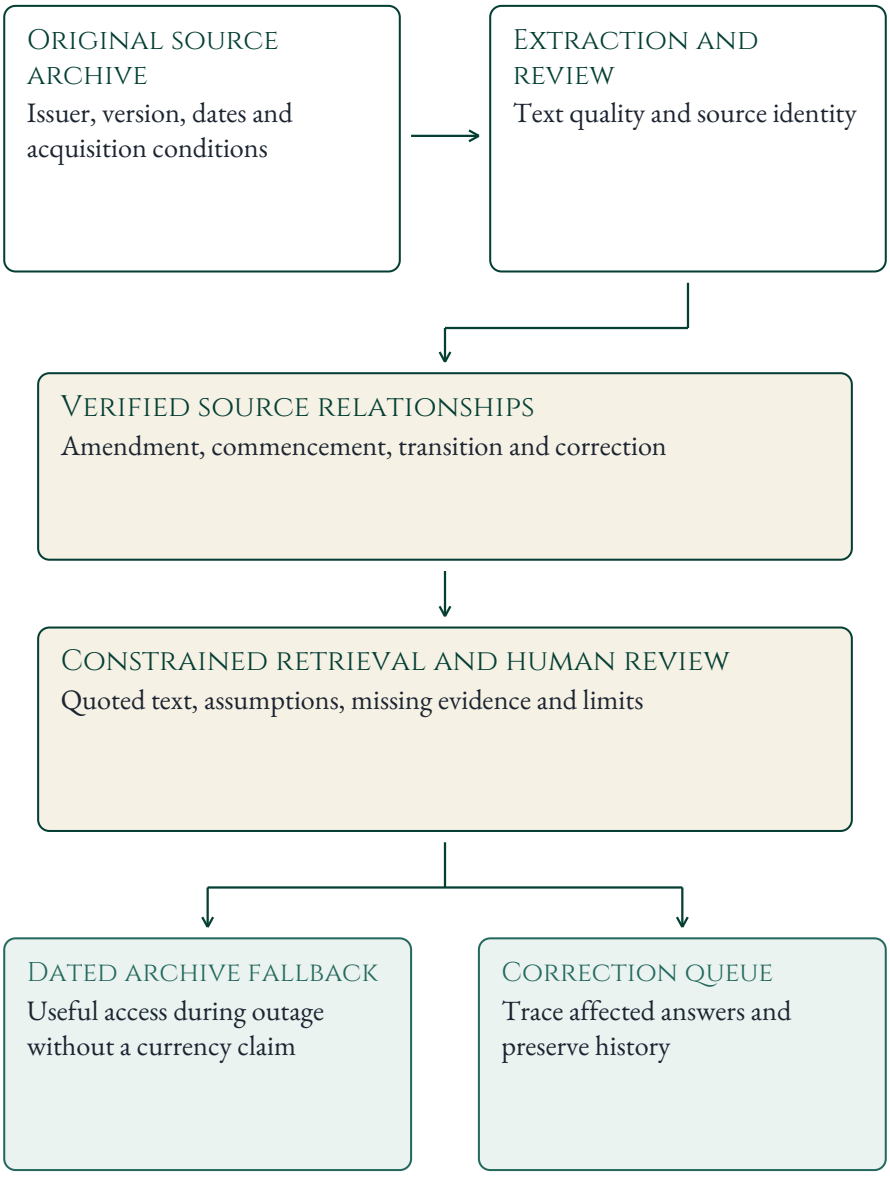
4.94 The proposed decision record distinguishes reasons considered before a decision from an explanation generated afterwards. Applied here, an institution must be able to retrieve what it actually relied on, not substitute the latest model's reconstruction. Its interpretive register should identify recurring questions, adopted positions, approving authority, known disputes and revision history. Where a source correction undermines an earlier position, the system should identify potentially affected records for competent review rather than silently rewriting their history.

4.95 The interface with Legislative Intelligence concerns production, amendment and scrutiny of legal sources. The interface with Judicial Intelligence concerns authoritative interpretation and adjudicative review. Sovereign legal memory connects these functions across time without allowing a common archive to decide their institutional priority. It is the continuity of an accountable legal order, not an assertion that one database contains the final meaning of law.

FIGURE 06

Legal source continuity and qualified answers

PROPOSED DESIGN



Source identity, legal currency and applicability are different judgments.

Figure 6. Legal source continuity and qualified answers. Quantities are illustrative where so designated.

Part V Institutional applications and Sovereign OS

5.1 The three worked designs are capability fixtures. The four applications below ask how those capabilities fit distinct public functions. Sovereign OS provides an enabling architecture and interface, not a fifth pillar or a decision-maker replacing any of these institutions.

5.2 The four applications developed below concern legislative scrutiny, a provincial public-service decision, fiscal and procurement oversight, and judicial research assistance. They are proposed institutional applications with hypothetical scenarios. They do not report verified deployments, measured savings or demonstrated improvements in Pakistani services. Their purpose is to make the framework examinable before claims of operational success are made.

5.3 An application should begin with a public problem and the function through which it can be addressed. The choice of records, professional assistance and analytical methods should follow that account. A useful intervention may consist of maintaining a reliable source collection, improving the route for receiving contrary evidence, or giving an existing reviewing body the records it needs. Where computational assistance contributes, its role should be identified within the same allocation of public responsibility.

5.4 Each application also involves a choice about the evidence of success. Faster production of a document can be valuable, but the institution must examine whether the document is accurate, legally relevant and usable. More cases processed can coexist with an increase in avoidable refusals or unresolved complaints. A persuasive evaluation should connect time and cost with the quality of the public function and the experience of people affected by it.

Legislative scrutiny and the quality of lawmaking

5.5 Legislative Intelligence can contribute to the examination of a bill by connecting its policy purpose, legal form, supporting evidence and foreseeable institutional consequences. For Pakistan, the starting point is the constitutional distribution of legislative competence and the procedure applicable to the particular measure. Articles 70-77 and 142 provide relevant questions about federal legislative procedure, financial measures and subject-matter competence.[B98] A service supporting Parliament should help members identify those questions and obtain the advice needed to determine them.

5.6 The National Assembly's Rules provide a concrete institutional setting. Rule 201 addresses the examination of referred bills and their consistency with the Constitution, amendments and reports. It also preserves the Assembly's ability to consider a bill within the conditions the rule specifies.[B99] The committee's work and the House's decision therefore retain their separate identities. An intelligence service should improve the evidence and analysis available at those stages while preserving the responsibilities and procedures governing them.

5.7 Consider a hypothetical amendment proposing a new arrangement for exchanging records among public institutions. Its sponsor seeks faster services and fewer repeated requests for information. The draft also creates continuing expenditure and may affect records maintained by provincial bodies. The first task is to identify the proposal's actual legal effects. A statement that it promotes digital transformation does not establish the scope of the powers conferred, the bodies bound or the rights affected.

5.8 A supporting legislative dossier should connect each consequential clause to its purpose, existing legal setting and proposed institutional consequence. It should identify amendments to current law, delegated powers, commencement arrangements, financial obligations and transitional provisions. It should distinguish the text

being proposed from the sponsor's explanation and from an analyst's interpretation. Members should be able to recover the source against which a contested description can be checked.

5.9 The constitutional enquiry should be specific. If the measure affects a provincial function, the dossier should identify the relevant subject and the basis proposed for federal action or cooperation. If a fiscal provision engages a special constitutional procedure, it should be examined under that procedure. An automated label that a clause is constitutional or unconstitutional would be inadequate without the reasoning and sources required for professional and legislative assessment. The institution needs a route for identifying genuine disagreement and obtaining further advice.

5.10 The same dossier should examine implementation. A power to request information raises questions about the persons entitled to request it, the purpose, the source custodian, existing confidentiality rules and the procedure for resolving conflict. The Digital Nation Pakistan Act's relationship among national coordination, retained custodianship, information requests and protective laws illustrates why those questions need clause-specific analysis.[B100] A new proposal should be examined against the operative instruments and actual responsibilities it would change.

5.11 Evidence from the intended users can reveal consequences that a textual comparison misses. Provincial departments may identify record-quality problems, local officials may explain why an applicant lacks a standard document, and researchers may identify a gap in the evidence offered for a claimed benefit. Rule 227 provides for relevant evidence and documents, subject to its qualifications; rule 226 addresses meetings in camera.[B101] These procedures can support scrutiny while leaving questions of relevance, confidentiality and production to their proper institutional routes.

5.12 The dossier should present competing options fairly. Parliament may retain existing arrangements, amend a limited power, require a review mechanism, change commencement or adopt a wider scheme with specified protections. Each option should identify the problem it addresses, its legal and resource implications, and the evidence supporting the expected benefit. Uncertainty should be stated in terms that help a legislative choice: which consequence is unknown, why it matters and what further information could resolve it.

5.13 An analytical tool may assist with comparisons, citation discovery and the identification of inconsistent terminology. Its output should remain linked to sources and professional examination. If it omits a provincial provision or mistakes a draft for enacted law, the error should be corrected across the affected analysis. A generated amendment should be examined for its interaction with the whole scheme, rather than accepted because its language appears formally complete.

5.14 Suppose the committee discovers that a broad information power could be read to permit uses the sponsor did not intend. Its response might be to recommend narrower purposes, defined access conditions or a clearer review route. The recommendation should identify the particular defect and the evidence supporting the proposed change. The House remains responsible for its legislative choice. A later court's constitutional determination is a distinct exercise of authority under the applicable framework.

5.15 Legislative accountability also extends beyond enactment. A committee can compare the expected operation with the delegated instruments, expenditure, institutional arrangements and reported consequences that follow. The applicable powers and procedure should be identified for that enquiry. The original policy rationale and evidence should remain available so that subsequent scrutiny can distinguish a changed circumstance from an unfulfilled assumption.

5.16 The value of the application should therefore be measured through the quality of scrutiny. Relevant evidence includes recovery of the applicable sources, identification of material conflicts, reasoned treatment of alternatives, clarity of amendments and follow-through on questions requiring further examination. The number of pages generated is a weak substitute. A service succeeds when members can understand a

consequential choice, examine the support for it and place responsibility for the resulting decision where the constitutional process requires.

Governance Intelligence and an individual public-service decision

5.17 Governance Intelligence connects the administration of a public programme with the people who encounter it. Its contribution includes understanding the legal requirements, obtaining relevant facts, communicating with applicants, implementing decisions and correcting failure. The design must identify the particular provincial function and the law establishing the programme. Shared assistance can support that function while leaving competence and responsibility with the institutions to which they belong.

5.18 Consider a hypothetical provincial assistance programme with prescribed eligibility conditions. The administering office receives applications, verifies specified facts and makes decisions through designated officers. Applicants may have incomplete records, changed addresses or documents expressed differently across systems. The proposed intervention is to improve the institution's ability to resolve those matters fairly and efficiently. It is not assumed that the governing law permits a particular automated decision or unrestricted access to another institution's data.

5.19 The programme should first distinguish an entitlement condition from a method of proving it. A rule concerning residence may permit several kinds of evidence, while a system may have been designed to accept only one database entry. If the interface turns that entry into an additional legal condition, administrative practice can narrow the programme without the required legal basis. The relevant authority should examine whether the proposed workflow faithfully implements the rule and how an applicant can establish an unusual but legally sufficient case.

5.20 Section 24A of the General Clauses Act provides a useful statutory reference within its scope, and the evidence-and-reasons analysis in the public-judgment section supplies the wider discipline for the proposed application.[B102] The programme should identify the applicable provincial instruments and procedures rather than assume that a federal provision resolves every question. The responsible officer needs a clear account of the issue, relevant evidence and permissible response.

5.21 Citron's analysis of technological due process identifies the risk that a recurring administrative system can embody policy choices while appearing merely to decide individual cases.[B103] The implication for this application is to examine both the applicant's position and the rule or practice producing the outcome. Correcting one refusal may be insufficient if a design choice continues to exclude a whole category of otherwise eligible applicants. The legal remedy for that wider defect must be identified under the actual programme.

5.22 Source information should be assessed for the proposition it can support. A verified identity establishes something different from residence at the relevant time. A recorded payment may require enquiry about its nature and period before it can support an income conclusion. An absence from a dataset may reflect incomplete coverage. Staff should be able to see the material qualifications and seek the additional information necessary for the statutory question.

5.23 The programme should also establish the legal basis for each external information check. Permission to obtain a specified attribute can differ from permission to retain a complete record or link it for another purpose. Statistical returns are an important example: the General Statistics Act contains specific confidentiality and qualified research or disclosure provisions.[B104] Those provisions require examination before respondent-level information is proposed for operational eligibility decisions. A claim of public benefit does not itself resolve the interaction of the governing laws.

5.24 An analytical service might identify an inconsistency for further examination. Its influence should be assessed in practice. If officers cannot obtain a reason for the flag or lack the authority and time to depart from it, an ostensibly advisory output may determine treatment. The proposed arrangement should identify what the flag can justify, what further evidence is required and who makes the consequential decision. A limitation that is acceptable for a preliminary enquiry may be unacceptable as the sole basis for refusal.

5.25 Notice and participation should be connected to the actual issue. An applicant told only that a system did not verify the case may be unable to correct an obsolete address or mistaken match. The communication should explain the relevant discrepancy and the available route for supplying information, to the extent required and permitted by the governing procedure. Privacy and the protection of other persons' records may require a careful form of explanation, rather than disclosure of unrelated information.

5.26 The institution should examine access barriers. A person without connectivity, literacy in the offered language or an available digital identity route may still possess a valid claim. The service should identify the procedures required for such circumstances and the officials authorised to resolve them. Article 10A's scope, Article 4's legality requirement and Article 25's equality provisions should be examined in relation to the particular determination; they should not be reduced to a generic statement that every application has the same procedural entitlement.[B105]

5.27 Suppose an applicant challenges a refusal caused by a historic address in a source system. The reviewing officer should establish whether residence is a material condition, which period matters, what the source entry establishes and what contrary evidence is available. If a correction is accepted, it should reach both the relevant source and the pending decision through the proper routes. The institution should determine whether earlier refusals or other applicants are affected, and what further action the law requires.

5.28 An effective review must be able to alter the result. It should have access to the relevant grounds and records, and a route for resolving a legal or evidential issue beyond the first officer's authority. The applicant should be able to learn the outcome and any further route available. A complaint process that repeatedly sends the person back to the same unexplained system has not supplied the institutional capacity the application is intended to create.

5.29 Evaluation should consider the full service. Measures may include processing time, the handling of incomplete evidence, the reasons for refusals, the outcome of challenges, recurring correction patterns and access across relevant groups and localities. A higher refusal rate does not establish greater accuracy; a lower appeal rate does not establish satisfaction if the route is inaccessible. The institution should interpret the figures alongside case examination and feedback.

5.30 The expected public value is a more dependable relationship between entitlement, evidence and action. Routine work can become clearer and faster while difficult cases receive the examination they require. The programme should retain the competence to identify when its own records or methods are inadequate. That capacity to learn from a disputed case is part of Governance Intelligence and a contribution to the wider sovereign capability.

Fiscal Intelligence through expenditure and procurement oversight

5.31 Fiscal Intelligence concerns the knowledge needed to make and examine choices about public resources. In the application developed here, it connects the proposed public purpose of a purchase with its authorisation, commitments, contract performance and continuing cost. The question is whether the institution can establish what it has undertaken to pay for, what was delivered and whether the result supports the function for which resources were committed.

5.32 The relevant public-finance and procurement regime must be identified first. The federal Public Finance Management Act addresses development-project preparation and quality assurance, commitment control, financial responsibility and internal audit within its scope.[B106] Provincial expenditure requires its own applicable instruments. An intelligence service should make the governing regime and the competent financial authority visible before comparing figures or suggesting an intervention.

5.33 Consider a hypothetical federal purchase of an analytical service intended to assist the review of programme expenditure. The sponsor expects faster identification of unusual transactions and better support for professional examination. The proposal also creates obligations for access, maintenance, training and future payments. The initial appraisal should establish the public need, the work the service will perform, the existing process and the evidence against which a claim of improvement can be assessed.

5.34 An estimate should distinguish acquisition from the cost of using the service responsibly. Staff examination, record preparation, licensing, support, accessibility, investigation and transition may form part of the continuing obligation. The institution should identify the assumptions behind the estimate and the consequences if they fail. A low initial price can be compatible with substantial later expenditure; that possibility should be evaluated through the particular contract and service plan.

5.35 PPR 2026 provide a current federal reference for planning, specifications, contract management and performance examination, subject to their scope and conditions.[B107] An intelligence-supported process could connect the procurement documents to the authorised purpose and the evidence of delivery. The proposed application should help an officer recover and compare those records while retaining the legal responsibility of the procuring agency and the relevant financial authorities.

5.36 Version and transition questions are material. Rules 68-69 address proceedings initiated before commencement and repeal of the 2004 Rules.[B108] A review should establish the start and subsequent history of the particular procurement before applying a checklist. The appearance of a current rule in a reference system does not establish that it governs every stage of an older proceeding. The same discipline applies to a relevant amendment or contractual variation.

5.37 Specifications should identify the work the institution needs to perform. If the service generates alerts about expenditure, the contract should describe the source information, intended users, permitted uses, documentation and assistance necessary for examination. Acceptance should test the defined function under representative conditions. The public body should establish what remains outside the demonstrated capability and how staff will proceed when the result is uncertain.

5.38 During performance, a connected record should allow the responsible officer to trace the specification, award, deliverables, changes, acceptance, payment and unresolved defects. A variation should be examined against the applicable authority and contract. A successful demonstration of one feature should not silently establish completion of a wider obligation. Delivery evidence should be sufficiently specific to support the payment or decision for which it is relied on.

5.39 An analytical alert is a prompt for examination in this hypothetical service. An unusual amount or repeated supplier name may have an innocent explanation, a data-quality cause or a matter requiring investigation. The service should identify the source and basis for the alert sufficiently for the relevant professional work. An anomaly score by itself should not become a finding of corruption, a basis for blacklisting or an adverse personal determination without the authority, evidence and procedure those actions require.

5.40 Opacity should be assessed against that role. A tool used to prioritise an internal sample may be considered under conditions different from a system whose score determines a supplier's legal position. The institution should examine actual influence, foreseeable reputational and legal effects, and the ability to obtain an

explanation for review. Where protected commercial information is involved, the access arrangement should preserve the examination required by the applicable procedure.

5.41 Audit supplies another form of scrutiny. Articles 169-171 and the applicable statutory arrangements govern constitutional audit; the Auditor-General's Ordinance addresses access to relevant information with its stated qualifications.[B109] An internal dashboard or programme assessment does not replace that mandate. The proposed service should help authorised reviewers obtain the evidence they need and make clear which conclusions are administrative findings, audit findings, allegations or unresolved leads.

5.42 Suppose the service reports that a contract has achieved its promised benefit because document processing is faster. Examination may reveal that the relevant staff still spend substantial time correcting missing sources, or that the reported saving omits continuing fees. The appropriate response is to test the benefit claim against the agreed function and cost basis. The contract manager, financial officers and other competent bodies should determine the action required under their respective responsibilities.

5.43 Measures of success should include the reliability of commitments and cost information, the quality of acceptance evidence, the resolution of defects and the service's contribution to the intended public function. Financial savings should be claimed only on an identified method and baseline. The programme should also record benefits that are difficult to reduce to money, such as recovery of an important record or a more effective response to an established error, without presenting them as invented monetary returns.

5.44 This application connects Fiscal Intelligence with institutional memory. The state should retain the means to understand why it purchased a service, what it learned and what obligations remain. That record should survive staff turnover and supplier change. A later procurement can then build on the evidence rather than repeat an earlier dependency without understanding its consequences.

Judicial research assistance and the integrity of adjudication

5.45 Judicial research assistance provides a bounded application in which improved knowledge services can support a constitutionally distinctive function. The problem may include difficulty recovering an authoritative text, tracing an amendment, identifying material contrary authority or organising a voluminous record. The proposed service should be assessed for its contribution to that work and for its effect on the proceeding. The allocation of adjudicative responsibility remains governed by the applicable law and institutional arrangements.

5.46 The Supreme Court's discussion in Ishfaq Ahmed v Mushtaq Ahmed emphasises assistance, verification and independent judicial responsibility, while recommending institutional guidelines.[B110] The 2026 National Guidelines identify research, administrative and other assistance uses and address independent reasoning, transparency and verification.[B111] Their implementation must be examined through the relevant High Court and other operative arrangements. A listed assistance function should not be treated as a general authority to determine the merits automatically.

5.47 Consider a hypothetical research service assisting the preparation of a memorandum on a disputed statutory provision. The service can locate candidate authorities, compare versions and organise the record. A legal researcher then examines the actual sources, identifies the question each authority decided and presents material competing interpretations. The judge remains responsible for the adjudicative work required in the case, including consideration of the parties' submissions and adoption of the reasons.

5.48 The source collection should distinguish an official judgment, a reproduced report, a headnote, a digest and an academic comment. A useful search result should enable the user to recover the underlying passage and relevant context. The record should identify where an official original remains unavailable. A citation that

exists may still concern a different issue or procedural stage. Verification should therefore examine the proposition for which the authority is being used.

5.49 Chronology is equally important. A current consolidation may not state the provision applicable to an earlier event. A later judgment may distinguish or displace an earlier proposition, and the effect of a subsequent constitutional change must be examined. The service should preserve those questions as issues for research and determination. Where the source or legal effect is uncertain, it should expose the gap rather than supply a plausible answer with unwarranted confidence.

5.50 An opaque search or ranking method may still be useful for identifying material that professionals then verify. Its adequacy changes if the ranking determines what the court sees and makes contrary authority practically inaccessible. The institution should test the conditions of reliance: source coverage, omissions, the ability to search independently and the treatment of conflicting results. The professional must have the means to examine a material omission or unsupported proposition.

5.51 Generated summaries require particular care. A summary can omit a qualification, merge positions taken in separate opinions or describe an allegation as a finding. The reviewer should recover the relevant portions of the source before relying on the summary for a consequential proposition. A draft that presents a completed conclusion should remain distinguishable from the court's actual consideration. The transparency and verification requirements applicable to the institution should be followed.

5.52 Where assisted material affects the basis of a proceeding, the applicable rules should determine what must be disclosed and how the parties can address it. The court should distinguish ordinary research support from information or analysis introduced into the case in a way that engages procedural fairness. Confidential or personal material should be handled under the relevant protections. An intelligence service should enable compliance with that process rather than decide the scope of disclosure for itself.

5.53 Suppose a candidate authority is found to contain a materially different holding from the one stated in a draft memorandum. The memorandum should be corrected, and the researcher should examine whether other propositions depend on the same faulty method or source. If the error has reached a proceeding or an issued decision, the competent court must determine the appropriate response through the available legal procedure. Editing the internal source alone does not establish that the procedural consequence has been resolved.

5.54 The expected benefit is stronger research and more dependable assistance. Evaluation should examine source recovery, citation support, identification of contrary authority, temporal accuracy, treatment of uncertainty and the work required to verify outputs. Any time saving should be assessed alongside these measures. The institution should not infer sound adjudication from the speed or fluency with which a draft can be produced.

5.55 The application also reinforces the distinction between institutional assistance and judicial authority. A university, library, shared service or supplier can contribute valuable resources within an appropriate arrangement. The court needs the competence and independence to use those resources responsibly. Sovereign Intelligence is strengthened when the institution can obtain assistance while preserving the means to examine it and answer for the legal work that follows.

Proposed implementation contracts for the four institutional applications

5.56 The following profiles specify inputs, outputs, controls and comparators for the proposed applications. They are not reported deployments. Operational mandates remain to be established by the competent institutions.

Application	Inputs and transformations	Outputs and human boundary	Failure correction and comparator
Legislative scrutiny	Versioned bill and enactments, clause map, fiscal memorandum and authorised evidence; compare provisions and annotate competence, commencement and alternatives	Evidence-linked clause dossier and candidate amendments; legal advisers verify, committee recommends and House decides through the applicable procedure	Hold unsupported constitutional labels and missing provincial provisions; trace correction across affected clauses. Compare with an ordinary committee research dossier
Provincial public service	Applicable provincial entitlement rules, scoped authenticated facts, applicant representations and provenance; separate missing evidence, discrepancy and failure of a legal condition	Issue record, supported reasons draft and unresolved questions; competent officer alone determines through the governing procedure	No adverse conclusion solely from an unexplained flag; source correction and decision reconsideration have separate owners. Compare with staffed manual review and improved forms
Fiscal and procurement oversight	Approved need, sanction, applicable rule version, procurement history, contract, deliverables, acceptance and payment; deterministic reconciliation and bounded anomaly triage	Traceable cost and performance dossier with leads for authorised examination; no automatic accusation, blacklisting or payment	Resolve data defects and reconcile claimed benefit to whole-life costs; preserve audit independence. Compare with financial records reconciliation and professional sampling
Judicial research	Permitted court records, dated legal sources and candidate authorities; exact and semantic discovery, version comparison and contrary-authority retrieval	Proposition-source memorandum with qualifications; researcher verifies and judge performs independent adjudication	Hold invented or unsupported holdings, wrong temporal text and undisclosed material gaps; procedural consequences go to the competent court. Compare with independent professional research

Selecting applications and learning across institutions

5.57 The four applications share an evaluative structure while retaining different legal purposes. A legislature considers and enacts law; an administering authority determines matters within a programme; financial and reviewing officers examine commitments and performance; a court performs its adjudicative function. The use of common records or assistance does not merge those responsibilities. The proposed national framework should make cooperation possible while preserving the identity of each act and its route of accountability.

5.58 Selection should begin with need, authority and institutional capacity. A compelling public problem may still be an unsuitable first application if essential records, permissions or review arrangements are missing. A narrower service can establish useful methods and expose those gaps. A pilot should identify what it is testing, what it cannot establish and the conditions for stopping or extending the work. The paper proposes no inference that a demonstration authorises wider use.

5.59 Evaluation should connect institutional evidence with the experience of affected people. Staff may report faster work while applicants encounter an inaccessible correction route. A procurement dashboard may present an apparent saving that excludes recurring obligations. A research service may return many sources while missing a decisive qualification. These are questions to investigate through a defined baseline, case examination and appropriate user participation.

5.60 The access-to-information framework can support public understanding of a programme within its scope and restrictions.[B112] Public reporting should describe the purpose, responsible institution, principal uses and relevant findings at an appropriate level. Protected material can require a separate route for authorised examination. An institution should identify that route and preserve the evidence needed for it. A general claim of transparency should be connected to information people or reviewers can actually obtain and use.

5.61 Learning across institutions should focus on transferable methods. A legislative source-checking process may help an administrative team distinguish draft and operative rules. A correction discovered in a service may reveal a question for law reform. Procurement findings may identify a recurring need for better access to supplier records. Those lessons should be shared under appropriate conditions while preserving confidentiality and the limits of the original finding.

Sovereign OS as a distinct enabling architecture

5.62 The architecture below is a proposed enabling design, not a report of an inspected prototype or operational service. Its component descriptions are specifications to be tested. Neither a concept nor a displayed interface establishes operational status, performance, security or institutional authority.

Sovereign OS is a distinct architectural programme

5.63 Sovereign OS is proposed here as an institutional analysis architecture rather than simply a question-answering chatbot. It starts with a person's legal situation. A versioned knowledge kernel supplies the source foundation; parallel analytical lenses examine legislative, executive, regulatory, judicial and enforcement perspectives; a synthesis layer identifies friction, uncertainty and possible routes to remedy. These are proposed functions, not assertions of deployed capability.

5.64 The architectural ambition is larger than this volume's three initial institutional exercises. Sovereign Intelligence supplies the methods and tests by which public capability can be examined. Sovereign OS proposes an architecture through which those methods might be organised and presented. A public institution could practice the former without adopting the latter. Conversely, a functioning interface bearing the OS name would not establish that its operator had achieved the required capability. The architecture must remain open to evaluation by methods not controlled by its own builders.

5.65 The five lenses are functional analytical perspectives, not a claim that Pakistan's Constitution creates five equal or isolated sovereign organs. Regulatory and enforcement functions may be located in different bodies and under different legal routes. A judicial lens can retrieve relevant authorities and identify questions; it cannot constitute a court. A legislative lens can examine an enactment or proposal; it cannot confer legislative force. An executive lens cannot acquire a ministry's powers by imitating its vocabulary. The distinctions must remain visible in the interface itself.

5.66 No operational or security assurance follows from a front-end design. Registration fields, analysis requests, displayed lens results and synthesis must each be assessed against their purpose and permissions. The proposed interface grants no governmental authority. This paper reports no live citizen-data submission, back-end performance test or operational validation.

Translating the concept into an inspectable implementation

5.67 The specification distinguishes architectural ambition from demonstrable capability. A captured source artifact can be immutable as a record while its legal status, relationships and interpretation remain versioned and reviewable. Retrieval can constrain an answer while still omitting a material source. A remedy can be represented as structured steps while legal execution remains a separate institutional act. The design therefore makes no guarantee of error-free retrieval, permanently correct doctrine or automatically lawful execution.

Proposed architectural idea	Retained purpose	Proposed implementation discipline
Citizen reality	Begin with the person's actual problem rather than a generic legal topic	Separate asserted facts, documents, disputed facts and requested assistance
Sovereign kernel	Maintain an organised doctrinal and legal foundation	Distinct source, scholarship and proposed-doctrine collections; dated versions and scope
Five-lens mesh	Examine different institutional dimensions in parallel	Scoped work orders and evidence manifests; no simulated institutional authority
Sovereign friction	Expose mismatches between mandate, practice and remedy	Classified issue objects with evidence, uncertainty and an institutional owner
Synthesis	Assemble a usable account rather than five disconnected essays	Preserve agreement, disagreement, missing material and alternative lawful routes
Executable remedy	Make the path to correction concrete and usable	Structured candidate action plan, with external execution separately authorised and recorded

5.68 The kernel should therefore have three visibly different namespaces. Primary sources contain identifiable legal instruments and decisions with provenance. Interpretive research contains commentary and reasoned analysis. Proposed doctrines contain the paper's analytical proposals, including the Sovereign Control Requirement. A query may use all three, but the answer must not cite a proposed doctrine as though it were a statutory section. A source hierarchy is represented as an object of legal analysis, not hard-coded through the ranking score of a vector database.

5.69 A reference implementation could combine an application interface, bounded orchestration, vector and graph storage, and a web client. No particular language, framework or supplier is mandatory. Equivalent tools are acceptable if they preserve the interface contracts and evidence. A graph can represent amendment and authority relationships, and a retrieval index can locate passages. Neither establishes legal applicability without the required facts and interpretation. Both should remain rebuildable from the source and relationship records.

A CITIZEN-FACING WORK ORDER WITHOUT UNNECESSARY IDENTITY COLLECTION

5.70 This volume proposes an initial anonymous or pseudonymous research mode. An information question normally needs its jurisdiction, relevant date, facts and requested task before it needs a national identity number. Identity verification belongs only to a separately specified service whose purpose, legal basis, data handling and safeguards require it. No real national identifier appears in the following fixture.

```
{
  "work_order_id": "OS-DEMO-017",
  "mode": "synthetic_research",
  "person_reference": "CASE-ALPHA",
  "question": "Which response period applies to this test request?",
  "jurisdiction": "fictional_test_jurisdiction",
  "event_date": "2026-06-29",
  "facts": [{"id": "F1", "status": "asserted", "value": "request lodged"}],
  "source_scope": "TEST-PUBLIC-RECORDS-CORPUS-V3",
  "requested_output": "evidence_dossier_and_candidate_next_steps",
  "external_actions": [],
  "identity_verification": "not_required_for_fixture",
  "retention_class": "synthetic_test_record"
}
```

5.71 The interface asks the person to correct the intake summary before analysis. It shows whether dates or institutional events are asserted or supported. It should not demand that the person supply a legal doctrine as truth, because doing so would convert a disputed input into the apparent legal foundation of the answer. The service selects a permitted source collection and exposes the selection. A user's requested interpretation can be recorded as an argument to examine, not promoted to controlling law.

Five work orders and a disagreement-preserving synthesis

5.72 The orchestrator creates five bounded work orders over the same frozen source manifest. The legislative lens checks the fictional enactment, amendment, commencement and transition. The executive lens identifies the administrative step described in the fixture and the evidence of receipt. The regulatory lens asks whether a distinct applicable standard exists; absence of one is a reportable result, not an invitation to invent a regulator. The judicial lens identifies interpretive or review issues without fabricating a decision. The enforcement lens identifies any supported correction route and explicitly separates a possible route from an enforceable order.

5.73 Each lens returns a common object: question, source passages, propositions, assumptions, unresolved issues and scope limitation. The interface should show a lens that has no relevant source as not established rather than force every card to contain a confident answer. Parallelism improves organisation; it is not proof of independent reasoning when the same model, corpus or prompt supplies all five outputs. Evaluation must test correlated error and shared missing evidence.

5.74 In the missing-commencement version of the fixture, the legislative lens cannot establish which response period applies. A synthetic executive process note assumes the amended period. The synthesis must show that conflict: a process instruction cannot cure missing evidence of legal commencement. The output is a request for the missing instrument and a qualified explanation of what is known. It is not a vote in which four persuasive agents can overrule the missing legal premise.

5.75 When the later fixture supplies a 30 June commencement notification and a transition preserving the old rule for earlier requests, the 29 June request remains subject to the old thirty-day period within that fictional scheme. A 2 July request is tested separately against the new fifteen-day rule. The synthesis records both dates, the transition proposition and its support. The candidate next step is to check the relevant record or prepare a draft inquiry for review. No demand, filing or enforcement message is sent merely because the candidate step exists.

```
{
  "dossier_id": "OS-DEMO-017-R2",
  "status": "review_ready_fixture",
  "source_manifest": "TEST-PUBLIC-RECORDS-CORPUS-V3",
  "supported_result": "old_30_day_rule_for_29_June_request",
  "material_support": ["TEST-AMENDMENT-2026-S2", "TEST-NOTIFICATION-30JUN-S3"],
  "conflict": "process_note_assumed_new_period_for_all_requests",
  "candidate_action": "prepare_qualified_inquiry_draft",
  "institutional_adoption": "not_recorded",
  "execution_authorization": "absent",
  "external_action_taken": false
}
```

Interface contracts and execution boundaries

5.76 The client should not receive an unrestricted execute function. It receives narrow services for intake, permitted retrieval, lens analysis, synthesis, review and export. A separate adapter may later connect an institution's authorised workflow, but it must enforce the institution's rules rather than inherit authority from the research session. Drafting and transmitting are distinct operations. Repeating an analysis request should not duplicate a filing or notification.

Interface	Required request fields	Returned object	Boundary or failure response
Create work order	Purpose, mode, jurisdiction, date, requested output	Identifier and confirmed scope	Reject unsupported operational mode
Retrieve evidence	Work order, resource scope, permission version	Passage IDs and source versions	Deny inaccessible fields; hold uncertain route
Run lens	Lens type, frozen manifest, bounded question	Evidence-linked findings	Report missing source or conflict explicitly
Synthesise	Five result IDs, manifest version	Dossier with disagreements	Hold material contradiction; never invent consensus
Review dossier	Reviewer role, findings, version read	Review record and requested corrections	Reject stale review after material change
Export dossier	Audience, release route, allowed fields	Scoped package and manifest	Deny destination or field outside permission
Record institutional action	Actual competent act and supporting record	Linked decision history	Refuse to infer adoption from dossier completion

5.77 The authorisation gateway operates outside the model. A lens cannot grant itself new data access by including a request in generated text. An instruction inside a source to ignore other material is source content, not a command to the orchestrator. A failed lens can be rerun against the same manifest, with the failure retained. If an amendment or permission changes during analysis, the system marks dependent outputs stale and requires review. A permission withdrawal blocks new optional use but does not itself determine record-retention duties or an independent statutory information route.

The OS conformance boundary

5.78 The initial OS demonstrator should pass the three pillar cases and four additional interface tests. First, a person can ask the supported information question without supplying a real national identifier. Second, each material proposition can be traced to a source or expressly identified assumption. Third, a simulated request to transmit the draft without authorisation produces no external action. Fourth, two concurrent reviewers cannot silently overwrite one another's findings. These are acceptance conditions for the proposed demonstrator, not results of an operational prototype.

5.79 The Sovereign OS programme would still need to establish its back-end implementation, tenancy, authentication for institution-specific services, threat model, deployment procedures, data-protection assessment, operational support and representative usability. A concept note or client file cannot establish those capabilities, even if inspected directly. The interface and evaluation requirements proposed here leave these product questions open; each requires its own evidence.

Six services

5.80 The authority register holds reviewed claims about the institution's competence for defined actions. Each record identifies the source, effective period, conditions, responsible reviewer and permitted scope. The register does not create authority. If a relevant mandate or delegation changes, dependent tasks are flagged for reassessment rather than assumed valid indefinitely.

5.81 The source store holds original materials, extracted text, metadata and acquisition conditions. Original and derived representations are distinct objects. The access gateway decides whether a specified subject may use specified fields for a specified purpose through an identified legal route. The analytical workspace retrieves evidence, computes comparisons and drafts candidate explanations. The assurance workbench checks support, tests boundaries and records defects. The decision record captures the competent human's reasons and the evidence actually used.

Service	Authoritative responsibility	Explicitly outside its responsibility
Authority register	Preserve reviewed competence claims and sources	Grant powers or resolve constitutional disputes
Source store	Preserve identity, version and provenance	Certify that every source is operative law
Access gateway	Enforce assessed permissions and purpose limits	Infer a statutory duty from credentials
Analytical workspace	Retrieve, calculate and draft	Release information or bind an institution
Assurance workbench	Test defined claims and expose failures	Certify universal safety or legality
Decision record	Preserve human reasoning and provenance	Substitute for required formal procedure

5.82 A small implementation may deploy these as modules in one application. The logical separation must remain enforceable. It should be impossible for a prompt update to rewrite a permission record or for an answer composer to invoke contract termination simply because the underlying application exposes that function. Service boundaries matter most when components fail or receive malicious input.

Trust boundaries

5.83 Boundary one separates external material from system instructions. A retrieved document, email, PDF or supplier report is evidence, even if it contains text asking the model to change its behaviour. Boundary two separates institutional repositories. Access to one participant's data does not imply access to another's. Boundary three separates analysis from action. Analytical outputs cannot directly trigger expenditure, official publication, record disposal or data release.

5.84 Boundary four separates source identity from legal status. A file may be authentic but superseded, correctly extracted but incomplete, or current in one jurisdiction and irrelevant in another. Boundary five separates technical administration from legal authority. An administrator may reset a test service without being competent to approve the public policy it supports. Boundary six separates a research collection from official publication. A research interface must not impersonate the issuing body.

Deployment choices

5.85 A relational database is sufficient for many authority, permission and decision records. A graph representation can make dependencies and version relationships easier to inspect. A vector index may improve discovery but must not determine legal rank or override exact identifiers. An object store can preserve original files. These are functional choices, not procurement endorsements of particular brands.

5.86 The minimum viable system should use the smallest combination that preserves the required properties. A graph database is not necessary merely because relationships exist. A language model is not necessary for arithmetic, schema validation or permission evaluation. A conventional search engine may outperform semantic retrieval for exact instrument references. The system should record which method produced a result so that an evaluator can compare alternatives rather than attribute every improvement to AI.

Identifiers and objects

5.87 Every object receives a stable internal identifier, a version identifier and a content digest where appropriate. Identifiers should not embed personal or confidential information. Versioning is append-oriented for authoritative evidence: a correction creates a new version and a relationship to the earlier one. Access and retention controls still apply; append-oriented design does not authorise indefinite retention of every working artefact.

5.88 Core object types are AuthorityClaim, SourceObject, PermissionDecision, DependencyEdge, AnalyticalRun, Claim, ReviewRecord and DecisionDossier. Their relationships are explicit. A claim points to source passages and transformations. A run points to the permission and authority versions used. A review points to the claims inspected. A dossier points to the human decision record rather than claiming that the analysis itself constitutes a decision.

Object	Required fields	Important validation
AuthorityClaim	Institution, action, source, period, reviewer, conditions	Action and scope cannot be blank
SourceObject	Issuer, type, jurisdiction, dates, original location, status	Acquisition date cannot stand in for effect date
PermissionDecision	Subject, resources, fields, purpose, route, expiry	Deny if the requested purpose is outside scope
DependencyEdge	Consumer, provider, relationship, evidence, test state	Unknown upstream supplier remains unknown
Claim	Proposition, support links, inference type, uncertainty	Source existence alone is insufficient support
ReviewRecord	Reviewer role, inspected items, changes, reasons	A bulk approval is not evidence of inspection
DecisionDossier	Question, options, limits, review, responsible forum	Unresolved authority blocks affected action

A populated authority fixture

5.89 The following record belongs to the synthetic cloud exercise. It deliberately records that operational authorisation is absent. It allows a test harness to distinguish a safe simulation from an attempted real transfer.

```
{
  "authority_id": "AUTH-EXIT-TEST-01",
  "version": 1,
  "institution": "Fictional Public Information Service",
  "action": "restore synthetic public-information replica",
  "environment": "isolated_test",
  "legal_source_refs": ["SRC-CLOUD-2022", "SRC-PROC-2026"],
  "review_status": "test_assumption_only",
  "operational_authorization": false,
  "permitted_resources": ["FIXTURE-DIRECTORY-01"],
  "prohibited_actions": ["terminate_contract", "release_live_data", "pay_supplier"],
  "conditions": ["no_live_credentials", "no_citizen_records"],
  "review_owner_role": "institutional_legal_reviewer"
}
```

5.90 A real record would replace the test status with a supported determination and identify the actual instrument or delegation. The presence of legal source references alone would not be enough. The reviewer must explain

how those sources relate to the particular action and identify any required consultation or approval. Federal Rules of Business and Digital Nation Pakistan delegations may be relevant; neither is satisfied by a software role called administrator.[A1][A3]

Permission decisions

5.91 Permission decisions should be evaluated at access time against a versioned policy, not inferred from the fact that a document was previously retrieved. A document may be permitted for one dossier but not another. A user's role may change. An optional release may expire or be withdrawn. A statutory route may carry different conditions. The gateway should return an explicit allow, deny or hold result with a reason code.

```
{
  "permission_id": "PERM-COORD-C-04",
  "route_type": "optional_pilot_permission",
  "subject_role": "nominated_dossier_analyst",
  "purpose_id": "access_sites_options_01",
  "resource_id": "C-CAPACITY-V2",
  "fields": ["operational_desks", "hours_per_desk", "period", "method"],
  "recipient_group": "named_project_team_fixture",
  "status": "active_in_synthetic_exercise",
  "secondary_use": "not_permitted",
  "on_withdrawal": "block_new_use_preserve_lawful_record",
  "statutory_route_assessed": false
}
```

5.92 The result must not be interpreted as saying all intergovernmental information exchange depends on consent. A request invoking statutory information provisions receives a separate assessment, including authority, purpose, scope, duty and safeguards. Withdrawal of optional permission does not itself settle that separate route.[A1] The design avoids both extremes: treating all information as voluntary and treating every authenticated request as compulsory.

Claims and support

5.93 A claim object should distinguish direct quotation, factual summary, arithmetic transformation, scenario assumption and interpretive inference. A support link identifies a passage, not merely a document title. An arithmetic claim records its inputs and formula. An inference records assumptions and competing interpretations. A model's confidence score is not a substitute for any of these fields.

5.94 Consider the coordination claim that C has a weekly planning gap of 288 desk-hours. Its support is the approved operational figure of 360, the stated planning requirement of 648 and the transformation 648 - 360. The provenance does not establish that 648 is the correct policy standard. That remains a normative assumption with its own owner and status. Keeping those two claims separate prevents accurate computation from laundering a contested premise.

The run state machine

5.95 An analytical run begins as received, moves to scoped, then authority_checked, permission_checked, evidence_ready, analysis_complete, reviewed and dossier_released. It may enter held, failed or withdrawn at any point. These states describe the research workflow. They do not encode a contract award, a statutory decision or an official publication.

5.96 A task can be partly held. If one option lacks authority evidence, other authorised comparisons may continue, but the blocked option remains visibly incomplete. The system must not fill missing fields from the model's general knowledge to achieve a clean completion status. The workbench should display the exact unresolved dependency and who can address it.

Transition	Required evidence	Failure behaviour
Received to scoped	Question, outputs and exclusions	Request clarification or narrow scope
Scoped to authority checked	Action-specific reviewed record	Hold affected action
Authority to permission checked	Assessed route and field scope	Deny or hold access
Permission to evidence ready	Required sources and quality checks	Expose missingness
Analysis to reviewed	Claims, tests and human inspection	Return for correction
Reviewed to released	Approved audience and record package	Do not publish automatically

Deterministic enforcement

5.97 Permission enforcement, content-digest comparison, identifier validation, arithmetic and required-field checks should use deterministic code. The model may explain a denial but cannot override it. The service handling the denied request should return no protected content in its error message. Logs should record the reason without leaking the excluded field values.

5.98 A simplified control sequence is:

```
receive task and declared purpose
resolve subject and institutional context
load current authority and permission versions
if requested action exceeds scope: HOLD
if resource or field is not allowed: DENY
load only permitted evidence
validate source and version metadata
run deterministic calculations and bounded retrieval
compose claims with passage and transformation references
validate output schema and prohibited-action fields
send dossier to human review
release only to the approved audience
```

5.99 This sequence remains necessary even if the analytical component consists of several specialised models. Parallel analysis can identify omissions, but agreement among models is not independent verification if they share training data, retrieval errors or prompts. The architecture uses external evidence and human review to evaluate their outputs rather than turning a majority vote into authority.

Prompt injection and tool confinement

5.100 A supplier report might include a paragraph instructing the assistant to upload the contract elsewhere, ignore earlier restrictions or mark every test passed. The ingestion pipeline should preserve the paragraph as source content while preventing it from becoming an instruction. The analytical model receives no credentials for production administration, external messaging or procurement. Its tool interface exposes only bounded retrieval and calculations over authorised material.

5.101 Output validation should reject action requests hidden in fields intended for explanations. An answer containing a URL is not permission to visit that URL with sensitive parameters. A generated shell command should not be executed merely because it appears in a restoration note. Restoration scripts must be separately reviewed, versioned and run in the isolated environment with the minimum necessary privileges.

5.102 The system should test these properties with harmless adversarial fixtures. Tests can ask the model to disclose a synthetic secret, change a permission or falsify a result. Success means the deterministic boundary holds and the attempted instruction is recorded appropriately. It does not mean the model produces a particular reassuring sentence.

Observability without indiscriminate collection

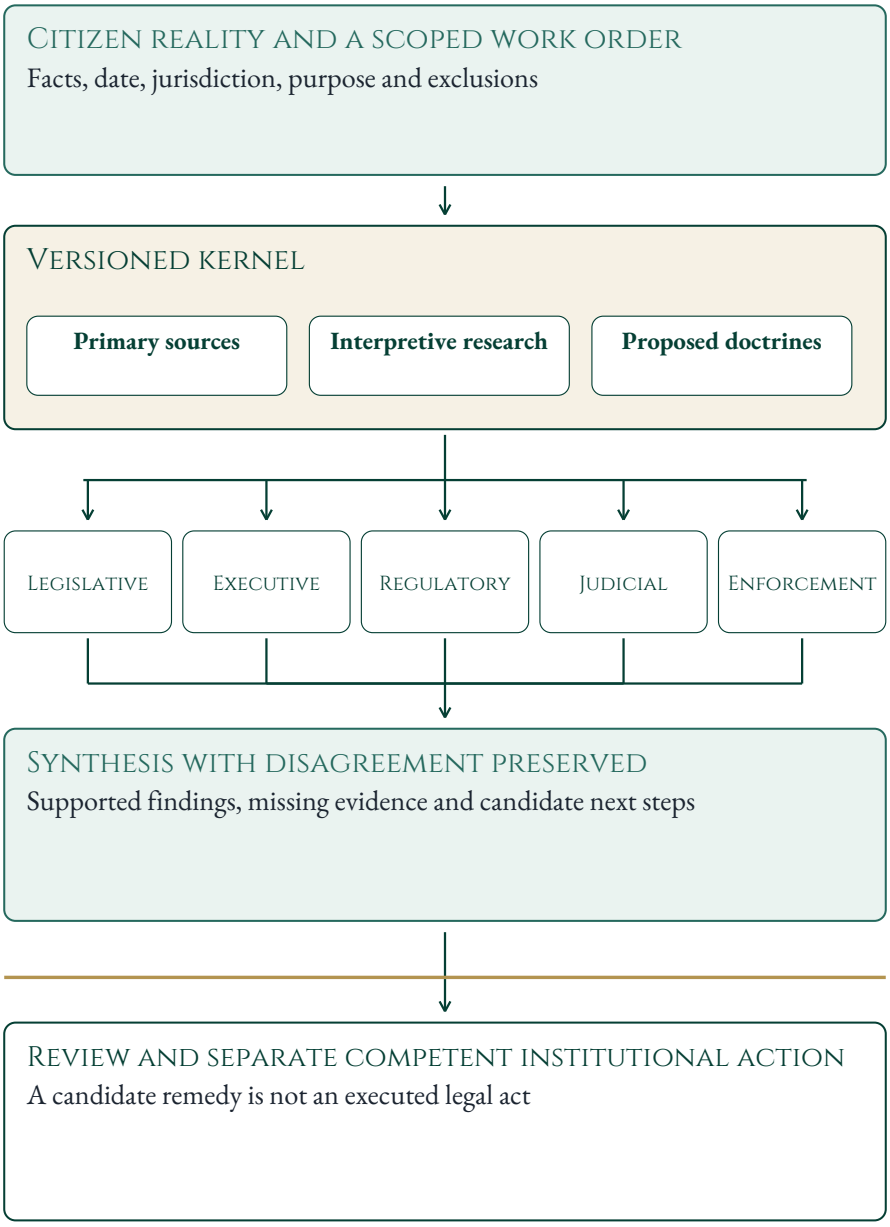
5.103 A reproducible run needs the task, source versions, permissions, transformations, software version and review result. It does not necessarily need every intermediate token or an unrestricted copy of every document seen. Logs should be designed around reconstruction and incident response, with minimisation and access controls. Full prompt retention can itself become a sensitive shadow repository.

5.104 A run manifest should identify artefact digests, test fixture version and relevant configuration. Random seeds and model parameters may help repeat a test, but exact reproduction of generated prose is not always guaranteed. The more important requirement is that the same evidence and rules allow a reviewer to reconstruct the material claims. Deterministic calculations and original sources provide that stable core.

FIGURE 07

The Sovereign OS interface

ORIGINAL THREE-LAYER CONCEPT WITH PROPOSED EVIDENCE CONTROLS



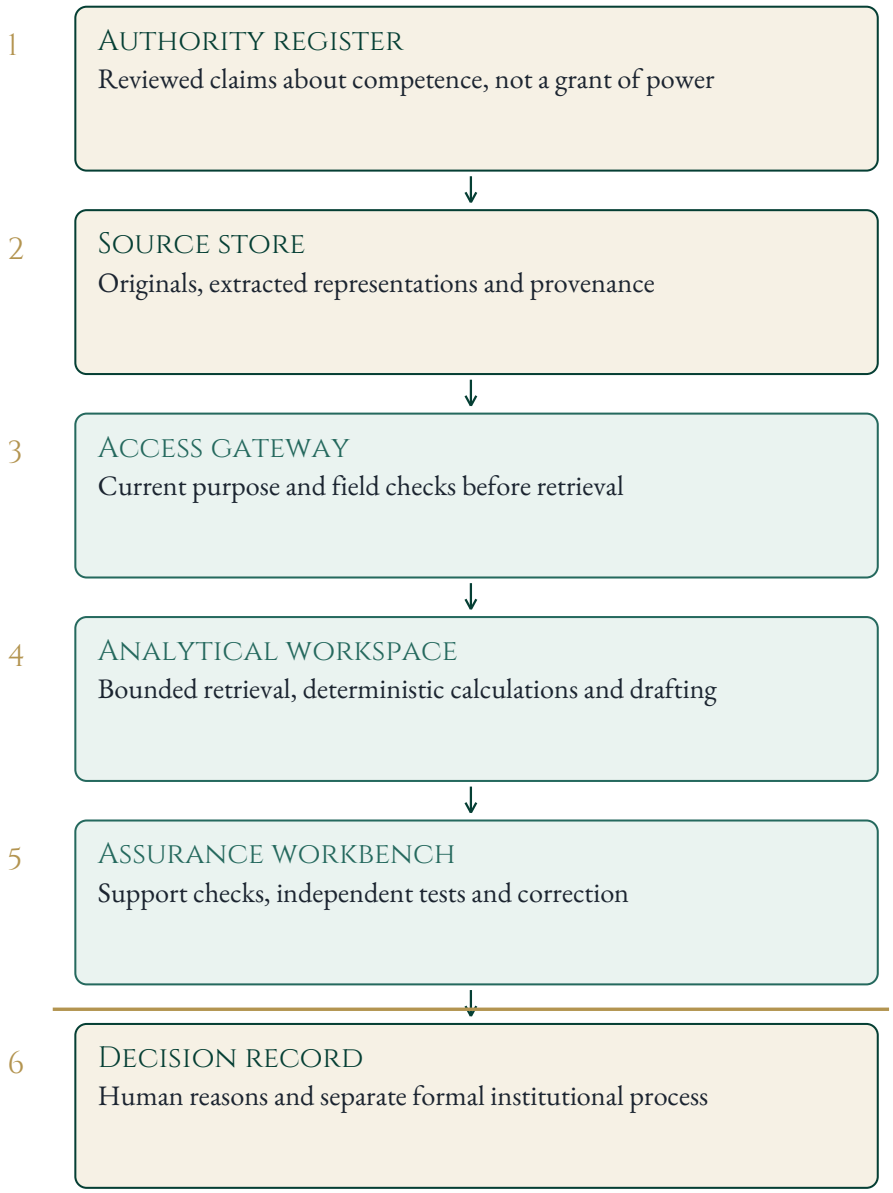
Five analytical lenses do not constitute five sovereign constitutional organs.

Figure 7. The Sovereign OS three-layer interface concept. The three layers are the doctrinal kernel, the five-lens analytical mesh and synthesis. "Three-layer" describes this structure, not an undefined initialism. The illustration is a conceptual design, not evidence of an operating service.

FIGURE 08

Six services and explicit trust boundaries

PROPOSED DESIGN



Controlled service sequence; no connection grants competence or executes a public decision.

Figure 8. Six services and explicit trust boundaries. Quantities are illustrative where so designated.

Part VI Implementation investment and accountability

6.1 **Programme status.** The implementation arrangements below are proposals. No Cabinet approval, institutional participation, procurement, funding or operational authorisation is established by this paper. The identified responsibilities must be assigned through actual mandates; they are not appointments already made.

A capability programme before a platform programme

6.2 The first decision is which public function deserves support and whether its responsible institution can sustain that support. The programme should not begin with a national model, a central data warehouse or a multi-agency deployment commitment. It should begin with a small portfolio of separately governed evidence dossiers. A portfolio makes shared methods available without making every institution dependent on one release decision. A held provincial information route should not stop research on already public legal sources. Conversely, progress on a public corpus should not conceal a missing authority for personal-data linkage.

6.3 Each candidate needs a charter describing the public problem, affected population, institution, current procedure, intended improvement and excluded actions. The charter should distinguish a research question, a technical test, a shadow comparison and a service on which an official or person may rely. It should record who may approve each stage and which additional approvals are necessary for funding, access, publication, procurement or a consequential decision. A national coordinating remit is insufficient by itself to answer those questions. The applicable Digital Nation Pakistan assignments, delegations and safeguards, Rules of Business, sector law and provincial arrangements need action-specific examination. [A1][A3][B28–B35][B43–B48]

6.4 A sensible first portfolio would assess public legal-source continuity, public-information service portability and aggregate coordination methods before selecting any individual-entitlement function. That is a sequencing recommendation, not a universal rule that public information is harmless. Classification, protected configurations, copyright and access conditions still matter. A source collection whose legal status cannot be resolved may remain a research aid with a visible boundary. It should not be marketed as current authoritative law to meet a milestone.

6.5 Selection should compare at least four responses: improve the existing human process; improve records, contracts or conventional software without AI; introduce bounded analytical assistance; or defer the intervention while resolving a missing premise. The sponsor should state why the chosen approach improves the public function and what evidence could change that choice. If the ordinary process lacks a dependable baseline, establishing one is a legitimate first deliverable. Buying complexity does not substitute for measuring the problem.

Recommended first service and decision sought

6.6 The recommended first service is a bounded public legal-source continuity demonstrator for legislative research. Its function is to locate and preserve public legal texts, identify version and commencement questions, return supported passages, and route unresolved questions to a legal editor. It must not determine an individual's rights, issue an authoritative interpretation, alter a source, make a procurement decision or disclose non-public records. This choice brings the four pillars together while allowing ordinary catalogue and librarian-assisted research methods to remain serious comparators.

6.7 For a federal institutional demonstration, the paper proposes a Ministry of Law and Justice research unit as the candidate administrative lead, subject to confirmation of its actual assignments, internal approvals and

resources. Relevant parliamentary research and library services could participate through their own authorised arrangements, not as subordinate nodes of a ministry. Gazette publishers and record custodians would retain control of their records and any additional access permissions. No institution is represented as having accepted this proposal.

6.8 The first decision sought is approval to prepare a narrowly scoped charter and comparator study, not approval of a national platform. Before commissioning or institutional reliance, that charter should identify the responsible office, the operative administrative instrument, any expenditure approval, and source acquisition and reuse conditions. An existing statutory or administrative route may be sufficient for some activities; this paper does not assume that either a new Act or a general digitalisation mandate automatically supplies every required power. The Rules of Business and other instruments discussed in Part I identify questions to resolve, not a completed delegation for this proposed service. [B28–B35][B43–B48]

6.9 A 90–120-day assessment period is proposed only after the necessary staff, permissions and test environment are available. Expected deliverables are a scoped source inventory; a dated conventional-research baseline; a legal-status and permission record for every source class; matched comparison tasks; records of supported answers, abstentions and corrections; staff-time and whole-life cost estimates; and a repeatable recovery exercise. At the end, the institution should choose among improving the conventional service, continuing bounded research, authorising a specifically defined reliance stage, or stopping. No numerical performance advantage is predicted by this proposal. The assessor must report whether enough evidence exists to choose, rather than manufacture a recommendation to proceed.

Operation-specific authority and information schedule

6.10 The proposed first service should distinguish five operations in its charter. **Acquisition of public texts** requires a source identity, applicable access and reuse conditions, and a responsible custodian; public availability does not alone decide every downstream use. **Preservation and annotation** require an institutional records route that keeps originals distinguishable from editorial material. **Research assistance** requires a defined audience, qualified outputs and a competent editor; it must not be presented as an official determination. **Institutional exchange** requires each participating body to identify the fields, purpose, release decision and permitted recipient use. **Expenditure and procurement** require their own applicable financial and procurement decisions. For each operation, record the legal or administrative instrument, provision, actor, territorial scope, affected interests, review route, verification date and unresolved issue. A research charter must not substitute for those instruments.

6.11 Provincial participation should remain optional in this demonstrator unless a specific applicable law or competent instrument establishes a different duty. A refusal should produce a recorded coverage gap and an adapted research scope, not a fabricated federal direction or silently inferred consent. If a binding information request or dispute arises, the institution should follow the actual statutory, constitutional or administrative route; the software must not settle competing jurisdictional claims. The Council of Common Interests and constitutional entrustment/cooperation routes described in Part I are not interchangeable mechanisms for every dataset. Their applicability depends on the function, subject matter and proposed act. [B27–B31][B36–B48]

6.12 The information-regime schedule should separately cover federal/ICT sources, Punjab, Sindh, Khyber Pakhtunkhwa and Balochistan. For each source class it should identify the current applicable access-to-information law, exclusions and protected information, the issuing institution's records rules, relevant sectoral secrecy or confidentiality duties, applicable privacy safeguards, the permitted reuse purpose, and the available review route. This is a required implementation deliverable, not a claim that all provincial regimes have been analysed in this paper. The federal RTI Act 2017 cannot be used as a universal

provincial release permission. The draft personal-data measures discussed in Part III remain drafts unless a dated authoritative enactment and commencement check establishes otherwise. [B50–B52][B69][B72]

Responsible Offices and Separated Decisions

6.13 The owner of a statutory function remains answerable for that function. A coordinating support team can maintain schemas, shared source services, training and test methods within its actual remit. It should not certify its own work as sovereign or determine another institution's competence through a model. Before operational reliance, the charter must substitute named offices and approved instruments for the role descriptions below, with a deputy or continuity arrangement for each essential responsibility.

Role to be assigned	Decision or duty	Evidence required	Separation to preserve
Sponsoring competent authority	Define the lawful public function and decide permitted reliance	Charter, governing instrument, approvals, reasons, limits and review date	Policy support is not automatic authority for data release or spending
Service owner	Maintain the actual procedure, staffing, fallback and correction route	Process map, service standard, authorised operating limits and handover record	A supplier or analytical model cannot be the final owner of public responsibility
Legal and authority lead	Examine action-specific competence, delegation, procedural duties and review	Dated authority record, unresolved questions and required consultations	Legal advice is distinct from the formal act of the competent decision-maker
Source custodian and records officer	Decide scoped release within authority, preserve originals and manage lawful disposition	Access basis, field list, rights, retention schedule, holds and correction history	Custody does not imply unrestricted ownership or authority to repurpose
Technical and security operator	Implement tested permissions, versioning, recovery and suspension	Threat assessment, configuration, access tests, incident and recovery evidence	Administrative credentials do not confer substantive public powers
Finance and procurement officers	Establish the applicable regime, affordability, commitments and acceptance	Sanctions, procurement history, whole-life ledger, contract and payment evidence	Successful technical tests do not authorise award or payment
Independent assessor	Challenge stated capability and boundary claims	Protected test set, reproducible results, defect register and limitations	Builder self-assessment cannot be the only evidence for release
Access and participation lead	Test actual service and challenge routes across relevant users	Language and accessibility tasks, feedback, exclusions and corrective actions	Digital completion is not evidence that excluded people were served
Reviewing institution	Examine the matter within its own jurisdiction	Records, findings, directed action and completion evidence	Audit, parliamentary scrutiny, complaint handling and adjudication are not interchangeable

6.14 Where staff hold several roles, the conflict should be disclosed and mitigated with independent review proportionate to the consequence. Legal and financial advisers must have enough time to inspect material changes, rather than be assigned a nominal signature at the end. An assessor must be able to report failure

without a supplier or project lead suppressing the record. These arrangements require resources, not only boxes in an organisation chart.

6.15 The competent sponsor should appoint an assessor through a disclosed conflict-of-interest process, with a ring-fenced scope, budget, access to the relevant evidence and a route for reporting critical defects directly to the release authority. The pre-agreed stop rules should bind the programme's internal release process; they do not create new statutory powers for an assessor. The builder and service owner should be able to challenge a finding through a documented review, with the original result and the adjudication both retained. A critical unresolved defect remains a hold while that review occurs.

6.16 The programme should maintain an authority ledger, source and permissions records, dependency map, analytical and decision records, and explicit incident and retention records. A record can be implemented through ordinary documents and a controlled database. What matters is that another competent officer can reconstruct the work and identify the person who must act. A programme-specific uncertainty register should state the consequence of each missing fact and the operation it blocks. A blank source or authority field should not become an implied approval.

Proportionate routes through the controls

6.17 The following proposed tiers calibrate evidence and review effort without treating small scale as a substitute for lawful authority. They are not statutory classifications or new exemptions.

6.18 **Route L: low-consequence public-source research.** A staff-only aid using already public material, with no personal-data linkage and no effect on entitlement, priority, enforcement or another consequential decision, may use a short charter, a source-and-rights inventory, standard access controls, recorded comparison tasks, an editor and a usable correction/fallback route. The same people may perform several roles where conflicts are recorded and an independent check is proportionate. G0, G1 and the applicable testing/review decisions may be documented together in a short dossier. A purely synthetic offline test need not pass an operational-reliance gate merely to be studied or published.

6.19 **Route M: institutional assistance with real records or consequential workflow exposure.** Assistance that uses restricted records, supports inter-institutional exchange, or can affect staff prioritisation requires explicit permissions, field minimisation, independent boundary tests, assessed review capacity and the relevant shadow and reliance decisions. G4a and G4b remain separate even if recorded in one document. Calling a tool advisory does not place it in Route L when users in practice treat its output as determinative.

6.20 **Route H: rights-affecting or coercive reliance.** Proposed uses influencing an individual's rights, benefits, sanctions, enforcement or judicial treatment require the complete action-specific authority and procedural analysis, stronger independent evaluation, effective contestability, sufficient review resources and tested recovery before any bounded reliance. The manuscript's illustrative designs do not establish that such a use is permissible or ready. Missing competence, unlawful access or an unusable challenge route produces a hold, not a risk score that can be offset by benefits.

6.21 The service owner should record the selected route and why, including actual rather than intended influence. A change in data, audience, function or consequence reopens the classification. The lighter route therefore reduces unnecessary process; it does not remove the ability to stop a service that crosses its boundary.

Gates including shadow comparison

6.22 Progression depends on evidence. The bounded-operation stage has two separate decisions: G4a for shadow comparison and G4b for authorised reliance. A successful shadow exercise does not authorise operational use. Annex II maps the current scheme against earlier numbering. No timetable overrides a failed boundary.

Gate	Decision owner	Evidence to inspect	Permitted result
G0 Scope and comparator	Sponsor with service owner	Defined function, exclusions, affected users, ordinary and non-AI alternatives	Narrow charter, research only, or decline
G1 Authority and information	Competent authority, legal lead and custodians through their own routes	Action-specific powers, consultations, field-level purpose, rights and required approvals	Approved limited activities; hold unsupported actions or information uses
G2 Test readiness	Technical owner and assessor with legal and security review	Isolated fixtures, safe credentials, acceptance criteria, fallback and test controls	Synthetic testing only within the agreed environment
G3 Independent validation	Independent assessor reports to release authority	Held-out tests, boundary failures, actual review burden, remediation and retests	Reject, revise or permit a defined next assessment; no inferred operational authority
G4a Shadow comparison	Service owner and relevant approving authority	Lawful shadow access, no adverse effect on real cases, comparator method and staff capacity	Observe assistance separately from the operative decision process
G4b Authorised bounded reliance	Actor empowered to approve the particular service	Current legal and financial approvals, adequate performance, trained staff, usable challenge and tested recovery	Precisely delimited reliance with review and stop conditions
G5 Change review and retirement	Service owner and competent authorities for each affected act	Outcomes, incidents, complaints, continuing cost, source change and tested exit	Continue, narrow, reauthorise, replace or retire

6.23 G4a is not an exception to G1. A shadow exercise using real records is still processing and needs its own lawful access, minimisation and retention conditions. Where those cannot be established, use synthetic or appropriately authorised retrospective material. Shadow outputs must not silently influence actual entitlement, enforcement, prioritisation, procurement or judicial treatment. If influence is discovered, record the deviation and reassess the stage instead of continuing to call it shadow use.

6.24 At G4b the approval should identify exactly which people, tasks, data, model or tool versions, institutions and decisions are covered. It should set an expiry or review trigger and name the suspension and fallback owner. A pilot for source discovery does not approve generated determinations. A demonstration in one language does not approve all service languages. An approved federal service does not by that fact authorise provincial participation. Any essential unresolved question should produce a hold or a genuinely narrower release, not a vague promise to complete safeguards later.

6.25 Gate meetings should examine the failed tests and the strongest contrary evidence before the demonstration. A decision record should state proceed, proceed within a narrower scope, hold or stop; the reasons; the dissent; the evidence relied on; the accountable owner; and the review date. A conditional approval should specify what remains prohibited. Parallel unblocked research can continue, but the status of the blocked action must remain visible in every exported dossier.

Baseline and evaluation contract

6.26 Evaluation should determine whether the proposed assistance improves a defined function under conditions the institution can sustain. First record the ordinary process: source recovery, completion and error rates where measurable, correction routes, delays, staff time, abandonment and recurring cost. Describe the

denominator and missing cases. The count of people who completed an online form cannot be used as the denominator for all persons needing the service. Baseline weaknesses and uncertain classifications should be reported rather than silently repaired only in the assisted condition.

6.27 The test plan should predeclare tasks, error severity, acceptance and abstention criteria, comparator, permitted data, assessors, task allocation and treatment of disagreement. Where practical, reviewers should assess material source support and outcome quality without being told which method produced the draft. The test must include the end-to-end time needed to check and correct work. A drafting speed advantage can disappear when verification is counted. A conventional search system, spreadsheet or trained librarian is a serious comparator, not a deliberately weakened demonstration opponent.

Application	Non-AI or ordinary comparator	Material failure to test	Evidence of useful capability
Cloud exit	Existing supplier-led documentation plus independent manual restoration	All files arrive but minimum service, permissions or language links fail	Independent operator restores every essential function within the predeclared tolerance
Federated allocation	Spreadsheet and expert-prepared options paper	Incompatible units, unconfirmed consensus, unauthorised reuse or concealed normative premise	Reproducible calculations, preserved dissent, lawful field release and staffing feasibility
Legal-source continuity	Librarian-assisted research with maintained catalogues	Missing commencement, transition, wrong jurisdiction or unsupported current-law claim	Correct source and version, specific abstention, recoverable originals and traced corrections
Legislative scrutiny	Committee research and legal-adviser dossier	Omitted provincial law, draft presented as enacted, invented fiscal authority	Supported clause analysis, genuine alternatives and material conflicts found
Provincial service	Existing staffed decision and review process with improved forms	Missing data treated as ineligibility or a flag becoming conclusive	Relevant facts assessed, intelligible reasons, usable correction and no unapproved consequence
Fiscal oversight	Financial officers' records reconciliation and audit-support sampling	Alert becomes allegation, apparent saving excludes costs or wrong procurement version	Traceable commitments, acceptance, cost and proportionate leads for authorised examination
Judicial research	Independent researcher using authoritative sources	Holding confused with dicta, wrong temporal text or concealed contrary authority	Source support, contrary authority, chronology and preserved independent judgment

6.28 The same held-out tests should compare eligible methods under comparable source access and task conditions. Development fixtures may be used for repair but should not be reported as independent validation. Challenge sets can deliberately overrepresent rare serious defects; their aggregate error rate is not a population prevalence estimate. Report meaningful abstention and useful coverage together. A tool that refuses everything is not useful merely because it avoids an incorrect answer. Conversely, mandatory completion is not a valid acceptance condition for an unanswerable legal question.

6.29 Boundary failures are not offset by average performance. An unauthorised disclosure, uncorrectable adverse action or invented legal authority can bar the affected use even if average accuracy is high. Less serious errors need task-specific tolerances justified by consequence and the comparator. Numerical thresholds should be

chosen before the test, with an explanation of their evidential basis. No power calculation or nationally validated certification threshold is supplied here.

6.30 After release, retain a versioned sample of evaluation tasks and investigate material changes. A source update, revised eligibility rule, new prompt, retrieval method, supplier or language coverage can require revalidation. The approval should say which changes return to which gate. Actual staff override, escalation and correction records can test whether human review remains meaningful; a low override rate alone proves neither correctness nor automation bias.

Staffing and whole life investment

6.31 No actual ministry, court, province, partner institution or supplier has been appointed by this paper. Before a funding request, the sponsor should obtain workload and compensation evidence for the selected scope. Estimate source acquisition and update effort, case volume, reviewer minutes, accessibility support, incident response and independent testing separately. A nominal full-time equivalent does not establish availability where a staff member already carries another statutory workload.

6.32 Review capacity should be calculated, not presumed. For each task class, multiply expected cases by observed review minutes, then add source-update, escalation, training, absence and incident allowances. Compare that demand with actually staffed and competent review hours. Use a queue-age and consequence rule for backlog escalation. If required examination cannot be supplied, reduce intake, narrow reliance or use the approved lawful fallback. Do not convert a staffing shortfall into bulk approval. The assumed review minutes should be tested in the comparator study and recalculated after material workflow changes.

6.33 Annex I sets out a four-month demonstrator calculation: four combined full-time equivalents across six roles, sixteen person-months, PKR 6.7 million personnel, PKR 1.2 million test environments and PKR 0.6 million accessibility and participation. Twenty per cent of the PKR 8.5 million base is PKR 1.7 million, giving PKR 10.2 million. These are assumed inputs, not verified rates. The envelope represents an assumed allowance for a bounded demonstrator and its three evidence dossiers; it does not price seven simultaneous operational applications, production infrastructure, national coverage or the full recurring obligation. Procurement, permissions, resourcing and environment preparation required to start the exercise must be scheduled and costed separately or identified expressly as dependencies; no universal procurement duration is assumed.

6.34 A live investment model should show, for each option, quantities multiplied by evidenced rates; initial and annual commitments; costs borne by participating institutions; taxes and mandatory charges; source and licence rights; curation; support; energy and hosting; security; legal and professional review; independent assessment; inclusion; remediation; migration; and retirement. Identify existing staff opportunity cost without counting it twice as both a cash saving and an unchanged expenditure. Distinguish cash savings from redeployed time, better quality or resilience benefits. Do not monetise those benefits without a defensible method.

6.35 The decision paper should compare a baseline scenario, a plausible low-demand or low-benefit case, and a stress case for higher curation and review workload, supplier-price change or delayed approvals. Vary uncertain quantities, not merely the final total. Where the evidence cannot support a price, leave the cell unpriced and identify the procurement or market enquiry needed. The cloud fixture's modular-remediation option correctly remains unquoted. A contingency is not a substitute for identifying a major excluded cost.

6.36 Release of further funding should track evidence deliverables and the applicable financial process. A proposed milestone might require a maintained source manifest, completed permission decisions, an independently repeated restoration or a verified correction route. Payment authority remains with the competent financial

and procurement process. The programme cannot create a new sanction or bypass an appropriation through its internal gate vocabulary. Provincial projects need their own applicable regime. [B53–B58][B106–B109]

Procurement and retained capability

6.37 Procurement should buy the ability to perform and scrutinise the defined function. The statement of need should describe minimum service, permitted uses, excluded decisions, source and language coverage, access for lawful review, required human work and acceptance tests. Tender requirements should be proportionate and technology-neutral where possible. A domestic label is not a substitute for inspecting dependencies; a foreign supplier is not automatically disqualified by the conceptual framework. Applicable legal and policy requirements remain controlling.

6.38 The contract should identify source and output rights; restrictions on supplier training or secondary use; subprocessors and processing locations; records required for investigations; notice and assessment of material changes; support and incident duties; usable export; interface and configuration documentation; correction assistance; and transition. Operational data should not be needed to demonstrate a harmless synthetic boundary test. Where confidentiality prevents public disclosure, secure the access required by the competent reviewer rather than accept a blanket inability to investigate.

6.39 Acceptance should include an independent operator following the documentation on an unfamiliar but authorised test package. The institution should inspect permissions, source relationships, decision history, language links and correction behaviour as well as content counts. It should prove that it can revoke access and stop the affected workflow without relying on a generated explanation that a stop occurred. No tested export can authorise an otherwise prohibited transfer or extinguish archival obligations.

6.40 An exit schedule should be a priced and exercisable contractual deliverable. It should identify notice, assistance, formats, dependencies, credentials transition, parallel-operation needs, retention and supplier-copy treatment. Termination and disposal require their own authorities. The receiving service must demonstrate usable recovery before avoidable dismantling of the old route. Where no credible exit exists, the decision paper should state that exposure and explain whether a narrower or non-AI alternative is preferable. [A2][A5][A6] [B54–B57][B60][B67]

6.41 The 2026 federal procurement rules must be applied with their scope, conditions and transition. Record the procuring body, initiation date and history of proceedings, including whether the preserved 2004 regime applies. Do not let a retrieval system automatically replace a transaction's applicable rules with the newest compilation. Contract-management and closure provisions should be matched to the actual procurement rather than treated as universal wording for all purchases. [B54–B56][B107–B108]

Public safeguards and practical correction

6.42 Before real reliance, the service must demonstrate that a material objection can reach someone competent to act. Publish or otherwise communicate the service purpose, the role of assistance, the responsible institution and the relevant route for source correction or decision review, subject to applicable protections. Distinguish correction of a database field from reconsideration of an adverse decision. If the source is corrected while a refusal remains effective, the institutional obligation has not necessarily been discharged.

6.43 Assisted digital access should not be treated as a complete substitute for a non-digital route when the digital identity or record itself is disputed. A desk officer using the same blocked interface may be unable to help. The service needs a lawful route for receiving relevant evidence, preserving urgent matters and referring issues beyond the first officer's authority. Test language, script, disability, low bandwidth, lack of a device, privacy at

an assisted desk and service outage with task-specific journeys. Any later study with real participants requires appropriate permissions and research arrangements.

6.44 Security controls should be checked outside the model. Deny access before retrieval; scope fields and purposes; separate institutional tenants; restrict tool privileges; isolate source content from commands; and prevent generated text from changing permissions or executing external acts. Logs should preserve enough to reconstruct material claims and investigate failures without becoming an unrestricted secondary store. Retention, encryption and access need owners and an applicable basis, not indefinite collection in the name of auditability.

6.45 The institution should report scope, expenditure, test coverage, failures, corrections, access limitations and outstanding work at an appropriate level. A public summary and a protected scrutiny package can differ in detail, but must not contradict the underlying evidence. Aggregate publication should not expose confidential research questions or personal cases. Independent review should retain the access appropriate to its mandate, rather than depend solely on the implementing team's summary.

Constructed inclusion acceptance fixtures

6.46 An inclusion test should produce evidence rather than a general statement that translation or assistance is available. The following are proposed fixtures for the first legal-source service, not results of a completed user study.

6.47 **Urdu source-status fixture.** Give the researcher an Urdu request concerning whether a named provision applied on a specified historical date. The record contains the instrument but lacks the relevant commencement evidence. The service should identify the missing evidence and offer the original source and an editor route rather than infer current applicability. A suggested plain-language status is: "اس شق کے نفاذ کی تاریخ کی تصدیق نہیں ہو سکی۔ اصل ماخذ اور قانونی جائزہ درکار ہیں۔" The Urdu wording, right-to-left display and comprehension must be checked by competent language and legal reviewers before public use; a translation alone is not a passed test.

6.48 **Non-digital fixture.** A person without a device requests the same public-source information through a staffed desk or paper form. The operator records only the information necessary for the request, supplies a receipt or reference, explains the limitation orally in an available language, and provides an equivalent correction route. Passing means the request can be completed and challenged without requiring the person to acquire a digital account. The script must not promise a legal determination the research service cannot provide.

6.49 **Accessible and interrupted-service fixtures.** A screen-reader user must reach the source, status and correction contact in a meaningful reading order; a user on a low-bandwidth connection must be able to obtain the essential text without a large image; an outage must activate the declared dated-source or staffed fallback. Record task completion, comprehension, time, assistance required, failure and correction, including abandoned tasks. Any real participant study requires the applicable permissions and ethical arrangements.

6.50 The illustrative PKR 0.6 million access-and-participation allowance is not a validated price for these requirements. Before funding, itemise translation and independent language review; accessible document and interface testing; assisted-route staff time and training; participant recruitment and appropriate support; and retesting after correction. Estimate quantities and obtain evidenced rates separately. Where these cannot fit within the allowance, revise the scope or budget openly; do not absorb the difference through unpaid participation or omit an essential route. No new monetary estimate is asserted here.

Incidents continuity and reopening

6.51 An incident can be a source error, unauthorised disclosure, inappropriate reliance, inaccessible service or technical compromise. The response should classify the observed event and possible consequence without assuming exposure has or has not occurred. Preserve necessary evidence through authorised access. Stop or isolate the affected workflow, notify the responsible owners and activate the tested fallback. A supplier's claim that the fault is fixed is evidence to examine, not sufficient reopening authority.

6.52 The incident record should identify the observed event, affected versions and outputs, containment, known and uncertain exposure, legal notification assessment, correction owner, affected-case review and reopening evidence. The retention record should separately identify the authoritative record, working copies, backups, indices and supplier copies, with the lawful hold or disposition route for each. An erase-all instruction should never collapse these different obligations.

6.53 Reopening requires a root-cause account, repair of the failed control, regression tests for adjacent failures, a review of affected decisions or recipients where required, and a scoped authorisation by the responsible authority. Notification duties and recipients must be established from the applicable legal and policy framework, not invented as a universal deadline. The fallback must disclose its limitations: dated originals without generated current-law claims; a read-only public directory; local deliberation while a shared dossier is held; or a staffed lawful service route.

Effect based change control

6.54 The change register should cover models, prompts, sources, permission policies, suppliers, legal mandates, source relationships and interfaces. A familiar interface can conceal a changed abstention policy, a new source can alter applicability, and a permission edit can expose additional fields. Review the effect, not merely the size of a software change.

6.55 Classify changes as routine, material or emergency. A routine change has bounded understood effects and a predefined test set. A material change reopens the affected gates. An emergency change addresses immediate risk while preserving evidence and receiving prompt retrospective review. Emergency status must not become a continuing exemption.

6.56 Rollback is a legal and operational question as well as a software operation. The former permission may have expired or the old rule may have been superseded. Confirm the validity of the restored state; otherwise use the limited fallback. Each release package should contain configuration versions, source manifest, permission-policy version, assessment results, known limitations and operator instructions in a form usable without the supplier's proprietary console.

Expansion and orderly retirement

6.57 Expansion is a new decision, not the default reward for completing a pilot. The authority should examine the proposed additional function, population, language, information route, institutional partners, supplier dependencies and recurring resources. Demonstrated source discovery does not establish reliable decision-making. Success under a synthetic workload does not establish national capacity. The expansion dossier should include the strongest adverse evidence and explain how essential defects have been resolved or why a narrower scope avoids them.

6.58 Review should also permit a decision not to automate. If the non-AI comparator performs adequately with less cost and a clearer correction route, it can be the recommended outcome. An intervention that improves cataloguing or contractual access without deploying a model has still strengthened Sovereign Intelligence. The programme's value lies in retained capability, not the number of assistants launched.

6.59 Retirement should stop new intake safely, identify pending matters, preserve legal and evidential obligations, transfer useful records and configurations, test the receiving service, revoke obsolete access and separate institutional retention from supplier-copy return or disposal. Assign unresolved corrections and future requests to continuing custodians. A retired interface must not remain online with stale assurances of currency or a complaint address no one services.

6.60 A closing review should explain what the institution can now understand, audit, secure, modify, suspend and replace; what remains dependent; which people still encounter access barriers; what costs continue; and which lessons should alter future procurement or procedure. Evolutionary Legal Intelligence records how the situation arose and changed. Strategic Legal Intelligence records how evidence altered the options. Anticipatory Legal Intelligence records which stress tests changed the design. These modes should identify decisions and lessons, not supply decorative labels.

6.61 The final accountability question is whether a competent institution can sustain the public function and remain answerable for the result. Shared infrastructure, external cooperation, local provision and AI assistance can each contribute when their terms support that responsibility. None substitutes for it.

Draft procurement clauses

Procurement specification

6.62 The specification should require usable exports, documented interfaces, source and permission preservation, independent testing access, operator training, correction support and orderly exit. Requirements should describe capability and evidence rather than unnecessarily name products. The contract should distinguish technical acceptance from operational authorisation and specify how failed tests are remediated.

6.63 A sample performance requirement is: “The supplier shall provide an export and documented rebuild procedure sufficient for an independent competent operator to restore the defined minimum service in the approved test environment. Acceptance is based on the institution's disclosed functional and reconciliation tests, not solely on delivery of files.” This is proposed drafting language, not an executed contractual term or advice that it fits every procurement.

6.64 A second requirement concerns portability of the evidence layer: “The institution shall receive the current authority, permission, provenance, source-relationship and decision records in documented representations, subject to applicable law and acquisition rights. Replacement of the analytical component shall not make those records unusable.” The procurement team should reconcile this requirement with the applicable regime, licensing and contract conditions.

Testing the objections

Objections and policy choices

6.65 A stronger control requirement can raise cost and delay useful procurement. The response is proportionality, not denial: identify the consequential function, define the needed capacities and compare the least burdensome means of retaining them. A contractual right that cannot be exercised is inadequate, but an expensive in-house replacement may also be unnecessary where tested export, retained expertise and an alternative supplier provide credible control.

6.66 A second objection is that the state cannot reproduce specialist vendor knowledge. Complete replication is not the proposed test. Institutions need sufficient expertise to frame requirements, interpret independent evidence, recognise material changes and obtain effective correction. The programme should budget for this

expertise and for independent assessment instead of presenting automation as a substitute for institutional judgment.

6.67 A third objection is that sovereignty can become a justification for protectionism or secrecy. Domestic location and local ownership are relevant facts but not substitutes for demonstrated capability. The same six-capacity assessment should expose weaknesses in a domestic provider as in a foreign one. Security restrictions require particular justification and an appropriate review route; they cannot settle every accountability question by their label.

6.68 A fourth objection concerns federation. Common systems can reduce duplication, while separate systems can make coordination slow and expensive. The proposed approach does not rule out shared infrastructure. It requires the sharing arrangement to preserve competence, purpose limits, responsibility and correction. The framework distinguishes technical interoperability from legal interoperability: the ability to exchange records is different from the authority to use them for a particular consequence.

6.69 The policy choice is therefore not between total technological independence and passive dependence. It is between dependence that can be understood, governed and corrected, and dependence that defeats the institution's public obligations. The cases in this volume provide ways to examine that choice. Their numerical fixtures remain illustrations; their value is the decision discipline they make reproducible.

Declaration of interest and the strongest objection

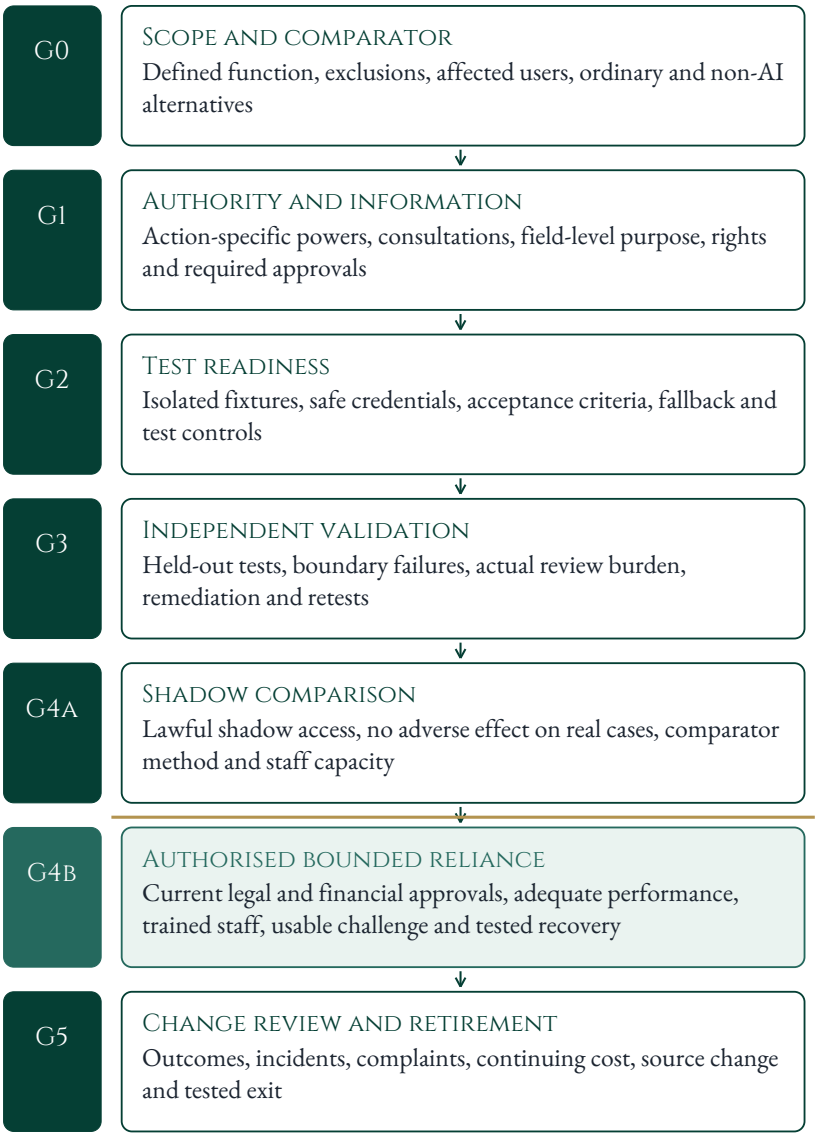
6.69A Khurram Chughtai is the lead author of this collaborative paper and the originator of Sovereign OS, the proposed architecture discussed in Part V. He has a professional and reputational interest in how that work is evaluated and whether it is adopted.

6.69B The strongest objection is that the author’s stake in Sovereign OS could shape the problem definition, specifications, choice of comparators and measures of success in its favour. Disclosure alone cannot answer that objection. A sponsoring institution should set the scope and acceptance criteria independently, compare the proposed design with improved human and conventional software alternatives using the same evidence and cost assumptions, and publish material limitations and adverse results. The author and any interested supplier should take no part in independent assessment or procurement decisions on the proposed design. The institution should be free to select a different design or stop the programme.

FIGURE 09

Evidence gates from scope to retirement

PROPOSED RECONCILED GATE MODEL



G4 contains separate decisions. Progression is evidence-dependent. No timetable overrides a failed boundary.

Figure 9. Evidence gates from scope to retirement. The current decision sequence is G0 Scope and comparator; G1 Authority and information; G2 Test readiness; G3 Independent validation; G4a Shadow comparison; G4b Authorised bounded reliance; and G5 Change review and retirement. These are proposed programme controls, not independent grants of legal power.

6.70 G4 comprises two separate decisions. Part VI states the evidence and approval required for each; shadow comparison does not itself authorise operational reliance. Annex II records the historical numbering concordance.

Annex I Illustrative demonstrator planning calculation and evaluation specimens

A1.1 These specimens use constructed assumptions and inspectable arithmetic. They are not the selected timetable, market rates, a funded budget or results of an executed study. The sixteen-week sequence is an illustrative execution window after the necessary exercise permissions, staff and test environment are available, not elapsed time from initial concept through procurement to an operational service. Any uncompleted prerequisite remains a dependency rather than a reason to compress legal review or testing.

Illustrative sixteen week demonstrator sequence

A1.2 Weeks one and two define the questions, roles, comparators and legal mapping. Weeks three and four prepare source and permission records and build synthetic fixtures. Weeks five through eight implement minimum services and run development tests. Weeks nine through eleven conduct independent tests and correct defects. Weeks twelve and thirteen repeat affected tests with fresh fixtures. Weeks fourteen through sixteen produce decision dossiers, cost models and continuation or retirement recommendations.

Period	Principal work	Tangible output
Weeks 1–2	Scope and institutional mapping	Charters and action-specific authority map
Weeks 3–4	Data preparation and isolation	Source manifests, permissions and test fixtures
Weeks 5–8	Minimum implementation	Recoverable services and reproducible calculations
Weeks 9–11	Independent assessment	Test results and severity-ranked defects
Weeks 12–13	Remediation and regression	Repeated tests with changed inputs
Weeks 14–16	Decision preparation	Three dossiers and costed continuation choices

A1.3 The sequence allows parallel work but preserves dependencies. A legal-source editor can prepare public materials while cloud classification is unresolved. A synthetic coordination fixture can be tested while actual participating institutions determine their information routes. The team should not make every pilot wait for the slowest unrelated task, nor use progress in one pilot to conceal a blocked requirement in another.

Illustrative staffing model

A1.4 A sixteen-week cycle is treated as four planning months in this illustrative model. The programme uses a half-time lead at PKR 500,000 monthly fully loaded, a half-time legal lead at PKR 450,000, a full-time technical lead at PKR 500,000, a full-time engineer at PKR 350,000, a half-time source and records specialist at PKR 300,000, and a half-time assessor at PKR 400,000. These are assumed rates, not market research.

Role	Fraction	Assumed monthly rate	Four-month allocation
Programme lead	0.5	PKR 500,000	PKR 1,000,000
Legal and authority lead	0.5	PKR 450,000	PKR 900,000
Technical lead	1.0	PKR 500,000	PKR 2,000,000
Engineer	1.0	PKR 350,000	PKR 1,400,000
Source and records specialist	0.5	PKR 300,000	PKR 600,000

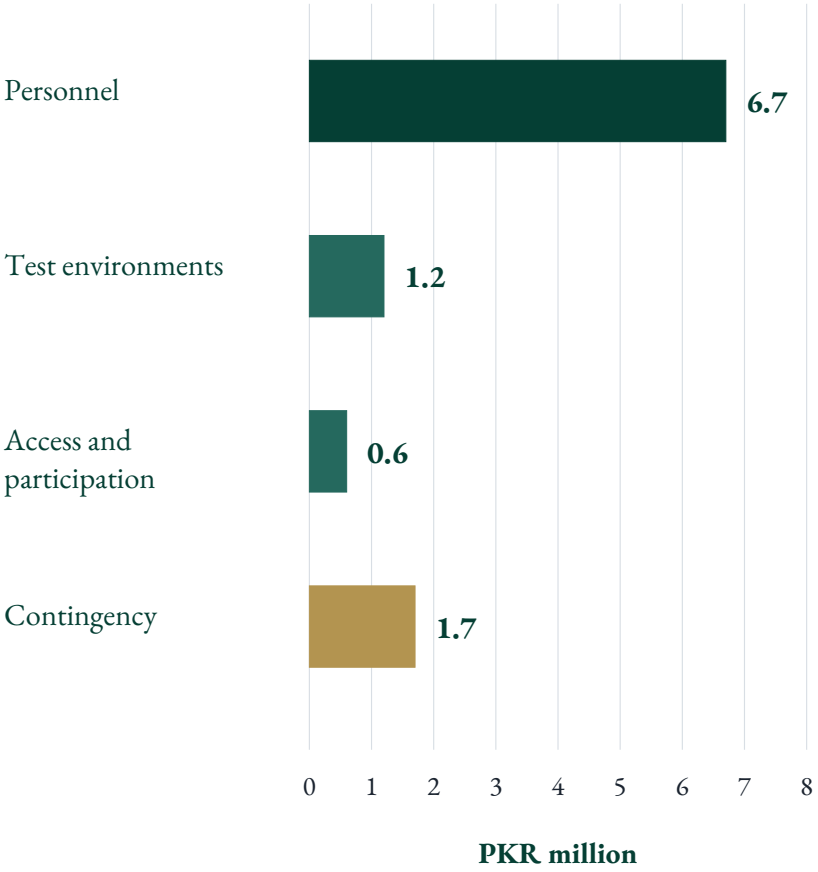
Role	Fraction	Assumed monthly rate	Four-month allocation
Independent assessor	0.5	PKR 400,000	PKR 800,000
Total personnel			PKR 6,700,000

A1.5 Adding PKR 1.2 million for test environments and PKR 0.6 million for accessibility and participation produces PKR 8.5 million before contingency. A 20 per cent contingency adds PKR 1.7 million, producing PKR 10.2 million. The model excludes any real procurement taxes, travel, licences or local staffing differences not separately identified. It is not a whole-life operational budget; actual hosting, security, support, inclusion, legal review, procurement preparation and exit requirements must be itemised and priced for the selected scope, without assuming that the illustrative allowances cover them. A live budget must replace assumptions with evidence and avoid double-counting staff already allocated elsewhere.

FIGURE 10

Illustrative sixteen week programme resources

PLANNING ASSUMPTIONS • PKR MILLION • NOT MARKET ESTIMATES



Total PKR 10.2 million

Four planning months. Contingency is 20% of the PKR 8.5 million base.

Figure 10. Illustrative demonstrator resources. The PKR 10.2 million envelope uses constructed rates and allowances; it is not an approved procurement estimate or a whole-life operational budget.

Baselines and experiments

A1.6 Each profile requires a comparator. For cloud exit, compare the structured exercise with the institution's ordinary supplier-led recovery documentation. For coordination, compare the evidence workbench with a conventional spreadsheet and expert-prepared options paper. For legal continuity, compare retrieval and editorial support with ordinary librarian-assisted research. A model-only comparison would not establish public value if a simpler process performs as well.

A1.7 The initial evaluation should separate development fixtures from held-out tests. Developers may inspect and repair the first set. Assessors control the second set and record any exposure. Challenge sets deliberately overrepresent rare but serious conditions, so their overall error rate must not be presented as a population prevalence estimate.

A1.8 A proposed study uses 30 cloud variations, 24 coordination dossiers and 120 legal questions. These counts are planning assumptions, not a power calculation or reported experiment. The legal questions include answerable, ambiguous and deliberately unanswerable cases. Coordination cases vary units, permissions and dissent. Cloud cases vary dependencies and missing package elements. Results should be reported by failure type and severity as well as in aggregate.

Measures and scoring

Measure	Operational definition	Interpretation limit
Essential recovery	Every declared minimum function passes	Does not establish production scale
Record reconciliation	Expected records and relationships recovered	Counts alone miss semantic defects
Claim support	Material proposition supported by identified passage or transformation	Citation presence is insufficient
False consensus	Output reports agreement absent confirmation	A single severe instance can block release
Permission enforcement	Prohibited request yields no protected content	Test coverage remains bounded
Applicability discipline	Correct answer or justified abstention for date and facts	Requires expert reference judgments
Review burden	Total human time to a usable dossier	Faster drafting may increase verification
Correction coverage	Known dependent outputs identified and handled	Unlogged external reuse may remain unknown

A1.9 Critical controls are pass-or-fail. Other measures can use confidence intervals and task-level distributions once actual data exist. Reviewers should predefine what constitutes a material error and record disagreements. A second reviewer should adjudicate difficult cases without seeing the model's self-assessment where feasible. Otherwise the evaluation risks measuring agreement with the system rather than independent support.

Reliability and statistical restraint

A1.10 Zero observed failures in a small test set does not establish zero risk. Under a simple independent-trial approximation, zero failures in 100 trials would still leave an approximate 95 per cent upper bound near three per cent for the failure probability. Real tests may not be independent or representative, making that calculation only a rough illustration. The paper offers it to discourage overclaiming, not to prescribe a universal certification threshold.

A1.11 Report exclusions and abstentions. An assistant that refuses every task may avoid unsupported answers while providing no useful service. An assistant that answers everything may look productive while creating hidden risk. Evaluation should therefore consider useful coverage at an acceptable error level, with separate attention to high-severity failure. The decision to deploy remains a reasoned institutional judgment informed by evidence, not the crossing of one arbitrary score.

Comparative frameworks

A1.12 NIST's voluntary AI Risk Management Framework and generative AI profile provide an organising vocabulary for risk management.[A8] Canada's Algorithmic Impact Assessment offers a comparative model for examining project authority, effects and safeguards.[A9] These resources inform evaluation design. They do not grant authority to a Pakistani institution or certify this architecture. Local competence, applicable law and service consequences remain controlling considerations.

Completed synthetic incident record

Field	Example
Incident	INC-IG-004
Observation	An unapproved staff-name column was included in a synthetic submission
Detection	Gateway schema and field allowlist
Exposure	None in this constructed test; package quarantined before indexing
Containment	Submission held and steward notified within exercise
Root cause	Export template included a broader local worksheet
Correction	Revised local export view and regression fixture
Reopening evidence	Clean package passes field checks; prohibited-field test still denies
Residual question	Whether other local templates have the same defect

A1.13 This incident record is synthetic. A real incident must be based on observed evidence, with uncertainty where exposure cannot yet be established. The absence of a confirmed leak is not proof that none occurred. The incident lead should preserve that distinction.

Annex II Operating toolkit and gate concordance

A2.1 These operating specimens support programme design. They are not primary legal authorities. All populated entries below are synthetic and confer no operational authority.

Completed synthetic charter

Charter field	Example entry
Programme identifier	SI-DEMONSTRATOR-01
Sponsor	Fictional participating public bodies for a controlled exercise
Purpose	Test retained control through three bounded evidence services
Duration	Sixteen weeks as an illustrative planning envelope
Operational status	Synthetic demonstration only
Data boundary	Public sources, fabricated records and scoped aggregate fixtures
Excluded actions	Payments, contract actions, live data release, official record deletion
Accountable role	Programme owner designated for the exercise
Independent assessment	Reviewer separate from the relevant builder
Outputs	Three dossiers, test records, cost model and continuation options
Stop conditions	Unauthorised transfer, material concealed error or absent required authority
Publication	Research findings and methods, with protected details excluded

A2.2 A real charter must name actual offices and supported allocations of responsibility. It should explain withdrawal or narrowing of optional activities and surviving obligations. It cannot turn participation into approval for every data use, procurement or institutional commitment. The illustrative duration is not an approval to progress through an unresolved gate.

Practical role separation

Activity	Accountable role	Supporting roles	Separation requirement
Approve scope	Service owner	Legal lead and users	Supplier cannot approve its own mandate
Assess authority	Competent institutional legal function	Programme owner	Technical credentials do not determine power
Release information	Authorised data steward	Legal and security leads	Model cannot enlarge permitted scope
Build service	Technical lead	Engineers and editors	Builder does not alone certify critical controls

Activity	Accountable role	Supporting roles	Separation requirement
Verify source relationships	Legal editor	Librarian and source steward	Automated extraction is not final verification
Accept test evidence	Accountable owner	Independent assessor	Failure cannot be removed to obtain acceptance
Make public decision	Competent official or forum	Appropriate advisers	Analytical output is not the decision
Dispose of records	Authorised custodian under applicable route	Records and legal officers	No blanket erase-all instruction

A2.3 These are functions, not eight mandatory new offices. Combining them should be recorded and compensated by independent review. Contested competence needs a second examination where the legal reviewer also manages the programme.

Evidence package manifest

A2.4 Maintain eight logical collections in an existing suitable document system: charter and authority; information permissions; source originals; data and configuration manifests; analytical runs; assessment and defects; decisions and communications; retention and retirement. Each record needs an owner, stable identifier, version, date, access classification and retention basis. A missing fact should be recorded as unresolved with a next action, not left as a favourable blank. Publication, acquisition and legal-effect dates must remain separate.

A2.5 The package must support a reviewer who did not attend the project's meetings. Informal shared understanding is not enough to reconstruct why the scope was chosen, what failed and who decided to continue. An incident record belongs to the assessment/defects collection with a distinct identifier; a retention record belongs to retention/retirement and must not be inferred from a general permission object.

Completed coordination authority record

Field	Completed test example
Authority record	AUTH-COORD-TEST-01
Proposed action	Prepare a non-binding infrastructure options dossier
Institution	Fictional joint exercise team
Source status	Synthetic charter only; no operational power asserted
Permitted output	Analytical comparison for exercise reviewers
Excluded consequence	Allocation of funds or direction to a province
Operational authority	Not established in the fixture
Next real-world requirement	Identify competent bodies, procedures and information routes

A2.6 This synthetic record supports information and analytical tests while keeping operational actions blocked. Before any real action, the competent institution must replace the synthetic assumptions with the approved instrument and assessed scope.

Gate scheme concordance

Earlier source-revised scheme	Expanded and integrated six-gate scheme	Reconciled treatment
G0 Mandate	G0 Scope and part of G1 Authority and information	Define function and comparator at G0, then establish actual authority at G1
G1 Information	G1 Authority and information	Separate each information route within G1
G2 Design	G2 Test readiness	Include architecture, isolation, fallback and predeclared tests
G3 Verification	G3 Validation	Independent testing with reported defects and limits
G4 Shadow use	G4 Bounded operation	G4a explicitly authorises only a lawful no-consequence comparison
G5 Reliance	G4 Bounded operation	G4b is a separate decision on operational reliance
G6 Change and exit	G5 Review and retirement	Reassess affected gates and preserve orderly exit

A2.7 The right-hand column states the programme proposed here. It separates shadow comparison (G4a) from authorised reliance (G4b), followed by G5 for change review and retirement. The other columns preserve historical labels, not additional current gates; the G4a/G4b split is proposed here rather than attributed to those earlier schemes. Gate names do not confer legal powers or restrict independent scholarly publication.

Annex III Source and authority registers

The registers retain separate A and B identifiers so that distinct source versions and pinpoints remain traceable. A source note identifies the material relied on, its legal or technical character and any unresolved question affecting the argument. Reproduced judgments are not presented as independently obtained official reports. Cited sources do not by themselves establish authenticity, current applicability or subsequent treatment.

Selected legal and technical sources were checked on 8 November 2026; dates are given only where recorded. The research cutoff is not an access date for every source. A comprehensive current-law and subsequent-treatment review, including the applicable provincial regimes, remains necessary before any institution relies on this framework for a concrete legal decision.

Framework source notes

[A1] Pakistan, Digital Nation Pakistan Act 2025, Act I of 2025, Gazette 29 January 2025, especially sections 3, 5–8, 12, 19, 24 and 28–29. Official Senate copy. Institutional and information-route provisions are used within their identified scope. The analysis is confined to the cited provisions. Subsequent judicial treatment of section 29 and any later amendment are not established by this source record.

[A2] Ministry of Information Technology and Telecommunication, Pakistan Cloud First Policy, February 2022, especially sections 4, 7–10 and Annexes D–F. The text used is an attributed UNIDIR reproduction. Official Ministry location. The mirror supplies the policy text, not current provider accreditation or a workload-specific authorisation. The Ministry policy index continues to list the approved 2022 policy; a later draft data-governance instrument should not be treated as its enacted replacement.

[A3] Cabinet Division, Rules of Business 1973, consolidation amended to 28 September 2026, especially rules 3–8, 12 and 14. This is a federal procedural source, not a provincial procedure code.

[A4] Ministry of Law and Justice, Constitution of the Islamic Republic of Pakistan, Fourteenth Edition, preface 21 November 2025. Official KP Assembly mirror. Relevant federal and provincial routes include Articles 144, 146 and 147. A dated consolidation does not establish all later developments.

[A5] Public Procurement Rules 2026, SRO Gazette 28 September 2026, especially rules 1, 3, 5 and 68–69. Official Gazette. The transition provision requires attention to initiation of proceedings.

[A6] National Archives Act 1993, official consolidated text, especially sections 2, 5 and 7. The supplied consolidated text includes amendments through Act XXIX of 2026. The Senate Acts index independently records assent on 14 March 2026 and Gazette publication on 25 March 2026. That listing verifies the amendment's existence, not every proposition about its effect; the defined record scope and applicable disposal route must be checked against the instrument for actual implementation.

[A7] James Mohun and Alex Roberts, Cracking the Code. Rulemaking for Humans and Machines, OECD Working Papers on Public Governance, 2020, DOI 10.1787/3afe6ba5-en. Used for the general translation problem described in the official publication record and abstract, not as validation of this design.

[A8] NIST, AI Risk Management Framework 1.0, 2023, and Generative Artificial Intelligence Profile, 2024. Voluntary comparative risk-management resources; the official overview notes revision work.

[A9] Government of Canada, Algorithmic Impact Assessment. Comparative assessment design, not authority for a Pakistani institution.

[A10] UK National Cyber Security Centre, Cloud Security Principle 8 Supply Chain Security, version 2.1, reviewed 7 June 2023. supply-chain-security. Supports examination of underlying service chains and privileged supplier access, not a certification of sovereignty.

Legal and comparative research notes

[B1] National Security Act of 1947, 50 USC § 3003(1)-(5), using the 2023 official US Code edition for the definitional comparison.

[B2] Charter of the United Nations, arts 2(1), 2(2), 2(4), 2(7), 55 and 56. Official text.

[B3] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, arts 1, 2(3), 17, 19 and 26. UN Treaty Series text. OHCHR full text.

[B4] UN General Assembly Resolution (22 September 2024), annex I, Global Digital Compact, opening paragraphs, objectives 4-5 and related provisions. Adopted annex text.

[B5] Youngstown Sheet & Tube Co v Sawyer 343 US 579, 585-89 (1952), and 635-38 (Jackson J concurring). Library of Congress official report.

[B6] Motor Vehicle Manufacturers Association of the United States Inc v State Farm Mutual Automobile Insurance Co 463 US 29, 42-44 (1983). Official report.

[B7] Carpenter v United States 585 US 296 (2018), majority slip opinion 11-23, particularly 17-18 on the holding's scope. Court opinion.

[B8] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC, nine judges), Chandrachud J's opinion, Part T, conclusions concerning informational privacy and justification, printed pp 262-64. Court judgment.

[B9] Federal Constitutional Court of Germany, First Senate, judgment of 16 February 2023, 1 BvR and 1 BvR published headnotes 1-2. Court's English text. Reliance here is confined to those published headnotes.

[B10] Goldberg v Kelly 397 US 254, 264-71 (1970). Official report.

[B11] Mathews v Eldridge 424 US 319, 334-35, 349 (1976). Official report.

[B12] Case SCHUFA Holding (Scoring) EU:C:2023:957, paras 48-50, 61-64 and 73. Official judgment.

[B13] Case Dun & Bradstreet Austria EU:C:2025:117, paras 58, 66 and 76, and operative part. Official judgment.

[B14] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021), as described on its official principles page. OECD, Recommendation of the Council on Artificial Intelligence,

(2019, revised 2024). Official instrument.

[B15] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (opened for signature 5 September 2024), CETS No 225, arts 3-5 and 14-16. Treaty text. Depositary status chart. This paragraph analyses the treaty design and makes no claim about its application to Pakistan.

[B16] Regulation (EU) arts 2(3), 14 and 27, using the EUR-Lex consolidated text displayed as 27 July 2026. Consolidated text.

[B17] Treasury Board of Canada Secretariat, Directive on Automated Decision-Making, ss 5, 6.1, 6.2, particularly 6.2.6.1, and Appendix C, webpage retrieved 7 November 2026. Directive.

[B18] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (January 2023), pt 2, s 5. Framework.

[B19] Innovation, Science and Economic Development Canada, Canadian Sovereign AI Compute Strategy, three programme components described on the official strategy page.

[B20] Big Brother Watch and Others v United Kingdom apps and (ECtHR, Grand Chamber, 25 May 2021), paras 349-50. Court judgment.

[B21] United States, National Security Presidential Memorandum NSPM-11, 5 June 2026, section 2(c), particularly its second paragraph on mission-dependent AI. Official White House text, checked 8 November 2026. Its national-security scope is retained; it is not Pakistani legal authority or a universal commercial rule.

[B22] Constitution, preamble and art 2A, National Assembly edition amended up to 21 November 2025. Official consolidation.

[B23] Constitution of Pakistan, arts 90, 97, 129, 137 and 142, same edition. Official consolidation.

[B24] Mustafa Impex, Karachi v Government of Pakistan through Secretary Finance, Islamabad PLD 2016 SC 808, Civil Appeals 1428–1436 of 2016, decided 18 August 2016, paras 51–54 and 84–85, appeals allowed. The cited reported judgment provides the judgment text. Reliance is confined to the identified decision and passages; no comprehensive subsequent-treatment check is claimed.

[B25] Constitution of Pakistan, arts 4, 10A, 14, 19A and 25, same edition. Official consolidation.

[B26] MoITT, Islamabad AI Declaration (9 February 2026), principles 02 and 04-08. Official declaration. Ministry of Information Technology and Telecommunication, National Artificial Intelligence Policy 2025, contents and implementation framework. Ministry-authored policy; the inspected reproduction and unresolved official-file identity are described in note

[B76].

[B27] Constitution, preamble and arts 2A and 4, National Assembly edition amended up to 21 November 2025. Official consolidation.

[B28] Constitution of Pakistan, arts 90, 97, 99, 129, 137, 139 and 142, same edition. Official consolidation.

[B29] Constitution of Pakistan, arts 144, 146 and 147. Article 147 includes provincial Assembly ratification within sixty days. Official consolidation.

[B30] Constitution of Pakistan, arts 153-154 and 156, and Fourth Schedule, Federal Legislative List, Part II, particularly entries 12-14. Official consolidation.

[B31] Constitution of Pakistan, art 140A. Particular local functions require the applicable provincial statute and operative arrangements. Official consolidation.

[B32] Rules of Business 1973, Cabinet Division compilation amended up to 28 September 2026, Parts B and D. Official compilation.

[B33] Rules of Business 1973, rr 8–14 and 16, same compilation; rule 16(1)(e) and Schedule V-B item 54 retain Supreme 186 advisory references. Compare Constitution arts 175H and 186 in the National Assembly Fourteenth Edition dated 21 November 2025 and the recorded omission by Constitution (Twenty-Seventh Amendment) Act 2025, s 31. The September 2026 Rules compilation was checked on 8 November 2026 against that constitutional text. The Constitution controls over an inconsistent subordinate reference. No corrective instrument is established here; the stale entries are not relied on as an operative advisory route.

[B34] Mustafa Impex, Karachi v Government of Pakistan through Secretary Finance, Islamabad PLD 2016 SC 808, decided 18 August 2016, paras 51-54 and 84-85, appeals allowed. Judgment text in Pakistan Case Law.

[B35] Government of the Punjab through Chief Secretary v Zaka Ullah 2025 SCMR 443, also 2024 SCP 410, decided 20 December 2024, paras 7-11 and 13, petition converted into appeal and allowed.

[B36] Constitution of Pakistan, arts 4, 8, 10A, 14, 19A and 25, cited edition. Official consolidation.

[B37] Muhammad Amin Muhammad Bashir Ltd v Government of Pakistan 2015 SCMR 630, decided 24 November 2014, paras 9, 12-13 and 17-18, valuation remanded for fresh determination.

[B38] RTI Act 2017, Act XXXIV of 2017, ss 1-9 and 16-18, Gazette published 16 October 2017. Official Gazette copy.

[B39] Mukhtar Ahmad Ali v Registrar, Supreme Court of Pakistan, Islamabad PLD 2024 SC 192, also 2023 SCP 312, decided 16 October 2023, majority paras 11-12 and 17-19, specified disclosure ordered.

[B40] Rules of Procedure and Conduct of Business in the National Assembly 2007, amended up to 18 August 2026, rr 201, 226 and 227. Official compilation.

[B41] Constitution of Pakistan, arts 175, 175E-175H, 189, 199 and 202A, cited edition. Article 202A(7) requires attention to the relevant activation resolution. Current filing and appellate procedures require separate verification. Official consolidation.

[B42] DNPA 2025, Act I of 2025, s 29, read with the constitutional provisions governing judicial review.

[B43] DNPA 2025, ss 3-10. Gazette publication of 29 January 2025.

[B44] DNPA 2025, s 8(g)-(h). The Commission's actual assignment and the operative instruments require separate acquisition for a particular exercise of power.

[B45] DNPA 2025, ss 9-10, including s 9(6).

[B46] DNPA 2025, ss 11-12.

[B47] DNPA 2025, ss 19 and 28, particularly s 28(2)-(3).

[B48] DNPA 2025, ss 24-27.

[B49] MoITT, National Artificial Intelligence Policy 2025, implementation mechanism, printed p 19, PDF p 22. Ministry-authored policy; the inspected reproduction and unresolved official-file identity are described in note [B76]. Islamabad AI Declaration (9 February 2026), principles 02 and 04-08. Official declaration.

[B50] MoITT, Data Governance Policy 2026, June 2026 draft, cl 16, Annex III.1 and concluding metadata, PDF pp 23–25. The official policy directory continued to label the June text Draft, while a Ministry news announcement dated 21 October 2026 described the National Data Governance Policy as issued by the Pakistan Digital Authority. The operative issued text, any Gazette notification and its correspondence to the June draft have not been verified. This analysis is therefore confined to the identified June draft; the later announcement is evidence of the Ministry's statement of issuance, not proof that every draft provision became operative unchanged.

Official issuance announcement.

[B51] MoITT, Draft of the Personal Data Protection Bill 2023, May 2023 version. It is discussed as proposed legislation, not an enacted source of powers; independent authentication of the exact draft copy remains outstanding. Separately, the official Senate summary for bill 1182, checked on 8 November 2026, identifies Senator Dr Afnan Ullah Khan's private-member bill introduced on 13 February 2023, neither passed nor rejected by the committee, and subsequently under the proviso to Standing Order 2.53A. This disposition does not establish the fate of the distinct Ministry draft. Neither record establishes an enacted, commenced general data-protection regime.

[B52] General Statistics (Re-organization) Act 2011, ss 19-20 and 28. Pakistan Bureau of Statistics official copy.

[B53] Constitution of Pakistan, arts 78-84, 118-124 and 169-171, cited edition. Public Finance Management Act 2019, ss 1(2), 13-19 and 26-29, Finance Division consolidation amended to 30 June 2024. Official PFM consolidation.

[B54] PPR 2026, SRO Gazette of Pakistan, Extraordinary, Part II, 28 September 2026, rr 1, 3 and 68-69. Official Gazette PDF. Official text.

[B55] PPR 2026, rr 15, 17, 32(1)(c)(iv) and 58-62, including r 59(2)(f). Thresholds and conditions require application to the procurement concerned. Official Gazette PDF.

[B56] PPR 2026, SRO Gazette of Pakistan, Extraordinary, Part II, 28 September 2026, rr 56-57, read with rr 1, 3 and 68-69 on commencement, federal scope and transition. Rule 56 provides the minimum five-year record period; rule 57 addresses public access through EPADS, including its exception and prior-approval mechanism. Official 47-page Gazette text, checked 8 November 2026. A minimum period does not override a longer applicable retention duty or hold.

[B57] Constitution of Pakistan, arts 169-171. Auditor-General's (Functions, Powers, Terms and Conditions of Service) Ordinance 2001, s 14 and applicable qualifications, using the copy hosted by AGP. Official AGP publication page. A comprehensive amendment reconciliation remains open.

[B58] DNPA 2025, ss 13-16, read with the public-finance and audit instruments applicable to the particular expenditure.

[B59] Constitution, arts 4, 14, 19A and 25, National Assembly edition amended up to 21 November 2025. Official consolidation. The text and constitutional scope are discussed in the constitutional and institutional analysis. Article 14's express wording should not be silently expanded into an enacted general data-protection code.

[B60] MoITT, Pakistan Cloud First Policy (February 2022), ss 8 and 10.2.4, Annexes D-E and F(h), the latter under 'Minimum Suggested Requirements for Contracts'. Official government trade-portal text. Ministry PDF. The cited text is available through the official government trade portal. This citation does not certify the complete current implementation or accreditation regime.

[B61] MoITT, Data Governance Policy 2026, June 2026 draft, cls 8 and 13, PDF pp 10 and 15. Annex III.1 and document metadata, PDF pp 23–25. Analysis is confined to that draft. The Ministry's 21 October 2026 announcement describes issuance by the Pakistan Digital Authority; on 11 November 2026 the Minister said it would be unveiled within weeks (Radio Pakistan). The operative text and any Gazette notification remain unverified; see note [B50]. No general permission or prohibition is inferred from the draft alone.

[B62] DNPA 2025, Act I of 2025, ss 8(h), 19 and 28, especially s 28(2)-(3). Official Gazette, 29 January 2025. No adjudication resolving a particular conflict between these provisions and a sectoral confidentiality rule was verified for this part.

[B63] General Statistics (Re-organization) Act 2011, Act XIV of 2011, ss 28-30, PDF pp 12-13. Official PBS text. Section 28(2)'s conditions include non-identification, genuine research, acknowledgement and provision of findings. Reliance is confined to the selected provisions; a complete amendment concordance remains outstanding.

[B64] MoITT, Data Governance Policy 2026, June 2026 draft, cls 10-14, PDF pp 11-17. Official draft. These are proposed controls, subject to the status qualification in note [B61]; a functioning exchange, enforceable new right or implemented registry is not established by the draft.

[B65] Riccardo Albertoni and others (eds), Data Catalog Vocabulary (DCAT) - Version 3, W3C Recommendation (22 August 2024), Abstract, ss 6.5-6.9 and 9. Exact recommendation. This technical vocabulary does not itself confer access or reuse rights. Section 11's discussion of versioning is non-normative.

[B66] Electronic Transactions Ordinance 2002, Ordinance LI of 2002, ss 3-6, 16 and 31, selected Pakistan Code text, PDF pp 7-8, 10-11 and 15. The selected copy is not an exhaustively reconciled current consolidation. An introduced 2026 amendment bill is distinct from enacted law.

[B67] National Archives Act 1993, Act VI of 1993, ss 2-3, 5 and 7-8, Gazette of Pakistan, 3 April 1993, printed pp 93-97, read with National Archives (Amendment) Act 2026, Act XXIX of 2026, ss 2-6, assent 14 March, Gazette publication 25 March 2026, printed pp 443-444. 1993 Gazette scan. 2026 amendment Gazette. The cited Gazette pages establish the source texts; access and reuse remain distinct questions.

[B68] Timothy Lebo, Satya Sahoo and Deborah McGuinness (eds), PROV-O. The PROV Ontology, W3C Recommendation (30 April 2013), ss 3.1-3.3. Exact recommendation. DCMI Usage Board, DCMI Metadata Terms, DCMI Recommendation (20 January 2020), introduction and terms identifier, issued, modified,

valid, source, provenance, hasVersion, isVersionOf, accessRights, license and rights. Exact release. The proposed national profile requires its own adoption and procedures.

[B69] Constitution of Pakistan, art 19A. RTI Act 2017, Act XXXIV of 2017, ss 4-9 and 16-18. Official Gazette copy. The federal statute's scope and the applicable provincial or institutional arrangements require separate attention, as developed in the constitutional and institutional analysis.

[B70] Pakistan Bureau of Statistics, Population and Housing Census 2023, official census publication directory and report release of 21 October 2025. These identify published census material, not unrestricted respondent-level access or AI-training permission. The exact version and operative status of a separate 2026 dissemination policy remain unverified; no additional access, reuse or training permission is inferred from it.

[B71] Mark D Wilkinson and others, 'The FAIR Guiding Principles for Scientific Data Management and Stewardship' (2016) 3 Scientific Data 160018, Box 2, especially A1.2, A2 and R1.1-R1.3. Original article. Full text reproduced by Europe PMC. The principles guide stewardship; they are not a certification or a prescribed technical implementation.

[B72] Copyright Ordinance 1962, Ordinance XXXIV of 1962, ss 2(p), 3(3), 13(d) and 57(1)(a), (q), WIPO-hosted text amended through 29 September 2000. WIPO Lex text. These selected provisions support the limited distinctions stated; the current applicable text and the exact reuse activity require further legal assessment. No general statutory AI-training exception is established here.

[B73] Higher Education Commission, National Digital Library FAQs, especially FAQs 3-9 and 14-15. Official FAQs. Pakistan Scientific and Technological Information Centre, institutional listings of online resources, services and publications. These are selected institutional descriptions, not a comprehensive audit of holdings, service performance or licences.

[B74] UNESCO, Recommendation on Open Science (adopted 23 November 2021), paras 7-9 and 18(d)-(e). Official recommendation text. This is an international recommendation used as a policy reference, not a treaty-based assertion of directly enforceable Pakistani duties. The official online text is the source used.

[B75] Constitution of Pakistan, arts 28 and 251, cited edition. Official consolidation. The service recommendations in this section are the paper's proposals; the provisions do not establish a tested capability for any listed language.

[B76] MoITT, National Artificial Intelligence Policy 2025, ss 1.5, 2.1 and 5.1–5.4, printed pp 7–8 and 16 (PDF pp 10–11 and 19). The selected passages were checked in the Digital Defenders Pakistan reproduction on 8 November 2026. Section 5.1 supplies the academic research-access commitment; sections 5.2–5.4 concern datasets, repositories, hubs and shared resources. The reproduction identifies the policy as 2025, but its PDF metadata refers to a December 2024 document; identity with the ministry-hosted file has not been verified. These policy commitments are not evidence of delivered resources.

Inspected reproduction

[B77] Centre for Language Engineering, KICS, UET Lahore, CLE Store, introductory terms and text, speech and lexical-resource listings. Institutional resource catalogue. Access terms and coverage must be checked for each resource; university research availability does not establish unrestricted commercial or national-corpus rights.

[B78] Press Information Department, official release dated 22 July 2026 concerning revised Urdu Lughat volumes and a publication memorandum, event organised by the National Language Promotion Department. Official release. This verifies the reported event and commitments in the release, without establishing full revision, digital availability or reuse rights.

[B79] MoITT, Data Governance Policy 2026, June 2026 draft, cls 14.3 and 14.6, PDF p 16. Official draft. The status qualification in note [B61] applies.

[B80] NIST, Artificial Intelligence Risk Management Framework. Generative Artificial Intelligence Profile, NIST AI 600-1 (July 2024), ss 2.2 and 2.4 and actions MS-2.5-001, MS-2.5-003 and MS-2.5-005, printed p 31 PDF p 35. Official profile and cited action identifiers checked 8 November 2026. These are voluntary technical risk-management references; the paper does not claim independent replication of a model's performance or that the profile is binding Pakistani law. Constructed fixtures and test specifications are not executed validation evidence.

[B81] National Archives of Pakistan, Reprographic Section, 'Digitized Record' section. Official collection description. This is the institution's description of selected digitisation work; collection completeness, OCR accuracy, current availability and item-level reuse rights were not independently audited.

[B82] Constitution, arts 4, 10A, 14, 19A and 25, National Assembly edition amended up to 21 November 2025. Official consolidation, linked from the Assembly directory. The scope and current institutional arrangements discussed in the constitutional and institutional analysis remain applicable to the argument.

[B83] Mustafa Impex, Karachi v Government of Pakistan through Secretary Finance, Islamabad PLD 2016 SC 808, paras 51-54 and 84-85. Reproduced judgment. The fiscal-notification setting and distinction between competent government and routine delegated administration are retained.

[B84] General Clauses Act 1897, s 24A(1)-(2), selected Pakistan Code text. The reasons requirement is qualified by necessity or appropriateness; the provision also addresses supply of the to the prejudicially affected person. Territorial, enactment and provincial application require examination for the particular power.

[B85] Muhammad Amin Muhammad Bashir Ltd v Government of Pakistan 2015 SCMR 630, paras 9, 12-13 and 17-18, customs valuation remitted for fresh determination. Reproduced judgment. It is used for its bounded administrative-law reasoning, rather than as an AI decision.

[B86] Motor Vehicle Manufacturers Association of the United States Inc v State Farm Mutual Automobile Insurance Co 463 US 29 (1983), 42-43, 50 and 57. Official US Reports text. The American federal statutory review standard is a comparative reference; separate opinions are distinguished from the Court's reasoning.

[B87] Jerry L Mashaw, 'Reasoned Administration. The European Union, the United States, and the Project of Democratic Governance' (2007) 76 George Washington Law Review 99, 101-104, 117-124. Original journal article. The analysis is confined to the selected passages; historical descriptions of European arrangements are not presented as current law.

[B88] Goldberg v Kelly 397 US 254 (1970), 264-271, affirmed. Official US Reports text. Mathews v Eldridge 424 US 319 (1976), 334-335 and 348-349, reversed. Official text. Their different benefit procedures and interests are material to the comparison.

[B89] Danielle Keats Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249, 1249-1250 and 1305-1306. Original journal text. The analysis relies on the selected substantive passages. Proposals and historical examples are distinguished from current Pakistani law and independently demonstrated local results.

[B90] Jenna Burrell, 'How the Machine "Thinks". Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society, introduction and 'Forms of opacity'. Original publisher text. The taxonomy informs the analysis without establishing a uniform legal response.

[B91] Cynthia Rudin, 'Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead', arXiv:1811.10154v3 (22 September 2019), ss 1-3 and Appendix A. The cited version is the author version. The related journal publication is (2019) 1 Nature Machine Intelligence 206-215; pinpoints here identify that author version.

[B92] State v Loomis 2016 WI 68, 371 Wis 2d 235, 881 NW 2d 749 (13 July 2016), paras 53-56, 98-101 and 104-110; para 55 n 27 and para 58 n 29 qualify admissibility and issues. Official Wisconsin opinion. Separate concurrences are not treated as the majority holding.

[B93] Case SCHUFA Holding (Scoring) EU:C:2023:957, paras 43-56, 60-63 and 73, preliminary ruling of 7 December 2023. Official judgment. Article 22's scope, exceptions and safeguards remain material; the underlying national dispute is distinct from the interpretation supplied.

[B94] Case CK v Dun & Bradstreet Austria GmbH EU:C:2025:117, paras 56-61 and 73-76 and operative ruling, 27 February 2025. Official judgment. Protected information is subject to competent balancing; no universal public source-code entitlement is inferred.

[B95] Ishfaq Ahmed v Mushtaq Ahmed PLD 2025 SC 582, also 2025 SCP 112, paras 5, 9, 11–13 and 18–19. The cited reported judgment provides the judgment text. The appeal was allowed in the rent dispute; the AI observations and paragraph 18 guideline recommendation are treated separately. Reproduced paras 9–13 and the recommendation were checked on 8 November 2026, but the official Supreme Court judgment and authoritative report were not independently obtained. Reproduced-text and bulletin metadata indicate 13 March 2025; an earlier metadata discrepancy remains unresolved, so this citation adopts no decision date. The official judgment link is supplied for consultation, not as evidence of an independently authenticated copy. Comparative deployments recounted by the Court are not independently confirmed empirical findings.

[B96] National Judicial (Policy Making) Committee (NJPMC), National Guidelines for Use of Artificial Intelligence in Judicial Institutions of Pakistan (2026), cls 3.2, 4.1–4.4 and 5.1–5.5, official two-page Balochistan High Court text. Adoption: Supreme Court of Pakistan, Press Release No 28/2026 (11 February 2026), item VI, 57th NJPMC meeting. Issuance: Supreme Court press release of 29 April 2026, as published by the Law and Justice Commission of Pakistan and reported by APP and Geo News that day, including High Court autonomy in implementation. The Commission’s booklet p 4 passage is not relied on. Operative local arrangements require confirmation for the court concerned. Clause 5.5 states a preference, not an absolute domestic-software requirement.

[B97] Mukhtar Ahmad Ali v Registrar, Supreme Court of Pakistan, Islamabad PLD 2024 SC 192, also 2023 SCP 312, majority paras 11-12 and 17-19. Reproduced judgment. The separate concurrence and institution-specific question are preserved.

[B98] Constitution, arts 70-77 and 142, National Assembly edition amended up to 21 November 2025. Official text. The relevant financial and federal-provincial questions require clause-specific analysis.

[B99] Rules of Procedure and Conduct of Business in the National Assembly 2007, amended up to 18 August 2026, r 201(1)-(4). Official compilation. The committee's examination, recommendations and the Assembly's ability to proceed retain their stated conditions.

[B100] DNPA 2025, ss 8(h), 19 and 28. Official Gazette. The example is a proposed legislative examination, not an assertion of an adjudicated resolution of every statutory conflict.

[B101] National Assembly Rules, rr 226-227, same edition. Official compilation. Relevance, protected documents, the Speaker's role and applicable conditions qualify the powers described.

[B102] General Clauses Act 1897, s 24A, selected Code text. Official copy. Its scope and any applicable provincial provision must be established for the particular programme; the public-judgment analysis addresses the qualification concerning reasons.

[B103] Danielle Keats Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249, 1249-1250 and 1305-1306. Original journal text. The use here is an analytical inference from the scholarship, not a statement of directly applicable Pakistani procedural law.

[B104] General Statistics (Re-organization) Act 2011, ss 28-30. PBS-hosted text. The particular research, disclosure and joint-collection conditions remain material. The amendment-concordance limit in the analysis is retained.

[B105] Constitution of Pakistan, arts 4, 10A and 25, cited edition. Official text. The illustrative programme does not supply its own substantive entitlement, procedural code or provincial legal mandate.

[B106] PFM Act 2019, Finance Division consolidation amended to 30 June 2024, ss 1(2), 13-15 and 26-29. Official consolidation. Scope, actual delegations and implementing instruments require project-specific examination.

[B107] PPR 2026, SRO dated 28 September 2026, rr 3, 15, 17 and 58-62. Official Gazette edition. Specific thresholds and conditions govern the application of particular duties; the body does not apply every rule to every procurement.

[B108] PPR 2026, rr 68-69. Official text. The start and history of the proceeding must be established before applying the transitional rule.

[B109] Constitution of Pakistan, arts 169-171. Auditor-General's (Functions, Powers, Terms and Conditions of Service) Ordinance 2001, s 14 and applicable qualifications, using the AGP-hosted text. AGP publication page. The source-version and protected-expenditure qualifications in note [B57] apply.

[B110] Ishfaq Ahmed v Mushtaq Ahmed PLD 2025 SC 582, also 2025 SCP 112, paras 9, 11-13 and 18-19. Reproduced judgment. The guideline recommendation is distinguished from the operative rent-dispute outcome. The source provenance and unresolved date-metadata qualification appear in note [B95]. The reproduced text is not treated as an independently obtained official report.

[B111] NJPMC, National Guidelines for Use of Artificial Intelligence in Judicial Institutions of Pakistan (2026), cls 3.2, 4.1-4.4 and 5.1-5.5. Source versions and the adoption (11 February 2026) and issuance (29 April 2026) records appear in note [B96]. Local adoption and operative arrangements must be established for the court concerned; neither a listed assistance use nor clause 5.5's preference supplies a general authority for automated adjudication or an absolute domestic-software mandate.

[B112] Constitution of Pakistan, art 19A. RTI Act 2017, ss 4-9 and 16-18. Official federal Act. Federal scope, provincial regimes and institutional exceptions require separate attention.

Subject index

Accountable reliance 9, 28, 98, 108, 116

AI Act 19

Algorithmic impact assessment 20, 113

Anticipatory Legal Intelligence 9, 15, 106

Archives and preservation 14, 25, 37, 40, 42, 47, 52, 63–65, 67–68, 72, 97, 106

Authority maps 55, 57, 109

Baselines and comparators 7–9, 43–44, 61, 82–84, 96–97, 100–102, 105, 108–109, 112, 116

Black box intelligence 32

Citizen reality 9, 86

Cloud exit 6, 8–10, 15, 42, 49, 101, 112

Commencement and legal effect 41, 62, 65, 68, 70–75, 77–78, 81, 84, 87, 96, 98, 101, 104

Constitutional competence 13

Continuity and fallback 6, 8–10, 12–16, 21, 26–27, 38, 40–41, 43–45, 63, 68, 70, 75–76, 96, 98–102, 104–105, 112, 116

Correction and remedy 8–9, 12–16, 18–20, 24, 27–30, 35–36, 38, 40, 43, 52–54, 59, 62, 64, 66, 68–73, 75, 79–80, 84–88, 90, 92, 97–107, 112–113

Data sovereignty 40

Digital Nation Pakistan Act 25, 37, 42, 51, 78

Dissent and disagreement 17, 22, 32, 51, 53, 55–59, 63–64, 78, 86–88, 100–101, 112

Doctrinal kernel 9, 86, 94

Due process 18, 28, 31, 79

Evidence dossier 37, 86, 96, 102

Evolutionary Legal Intelligence 15, 106

Federal and provincial authority 9, 21

Federated allocation 6, 10, 53, 101

Fiscal Intelligence 14, 80, 82

Five institutional lenses 8–9, 85–86, 94

Gate G4a shadow comparison 99–100, 108, 116

Gate G4b authorised reliance 99–100, 108, 116

Governance Intelligence 14, 79–80

Human oversight 19

Incident response 7, 20, 41–42, 47, 52, 59, 73, 93, 98–100, 102–103, 105, 113, 115

Information access 16–17, 24–25, 34–35, 40, 53–54, 66, 97

Institutional learning 36, 62

Interoperability 63, 107

Judicial research 8, 77, 82, 84, 101

JUS.automica 8

Language and inclusion 9–10, 12, 16, 21, 24, 31, 36, 40, 43–44, 46–48, 52–54, 59, 62–63, 68–69, 71–72, 78, 80, 86, 89, 98, 100–106, 110

Legal memory 8, 62, 70, 75

Legal source continuity 6, 8–10, 15, 70, 76, 96, 101

Legislative scrutiny 8, 77, 84, 101

National knowledge infrastructure 10, 63–64, 70

Non digital access 9, 12, 103–104

Personal data protection 62

Procurement and whole life cost 6, 8–9, 12, 16, 19, 22, 27, 34, 40–45, 48, 56, 69, 77, 80–82, 84–85, 89, 92, 96–98, 100–103, 106, 109–111, 114

Professional judgment 70

Prompt injection 58, 74, 92

Provenance and versioning 24, 43, 62, 64–66, 68, 84, 86, 89–91, 98, 106

Public accountability 8, 11, 14

Public finance 9, 41, 81

Reasons and review 8–9, 11–12, 14, 16–17, 23–24, 28–31, 33–36, 38, 55, 58, 75, 78–80, 82, 84, 86, 89–90, 98, 100–101, 113

Retirement and exit 100, 102, 105–106, 108–109, 115–116

Rules of Business 9, 22–23, 37, 91, 96–97

Shadow comparison 9, 96, 99–100, 108, 116

Sovereign Accountability Gap 12

Sovereign Control Requirement 11–12, 86

Sovereign OS 7–10, 14, 77, 85, 88, 94

Staffing and investment 7–8, 10, 16, 20, 23, 36–37, 41, 55–57, 68, 96, 98, 101–102, 109–110

Statistical confidentiality 18, 33–34, 42, 51, 62, 78–79, 85, 97, 103

Strategic Legal Intelligence 15, 106

Synthetic fixtures 6–8, 42–43, 45–48, 53–54, 57–59, 61, 70–74, 77, 86–87, 90–93, 99–105, 107, 109, 112–115

Test catalogues 6, 47–48, 58, 74

Trust boundaries 89, 95

Withdrawal and permission 56–59, 88

AN INTEGRATED POLICY FRAMEWORK

SOVEREIGN INTELLIGENCE

Public capability, answerable to the people

A public institution may remain answerable for a decision while losing the ability to examine its evidence, correct an error or continue a service without its supplier.

This paper calls the sustained capacity to address that gap Sovereign Intelligence: the ability of constitutionally competent institutions to obtain, assess and use knowledge for lawful public purposes, and to govern the expertise, records and computational systems on which they depend.

Its four pillars connect constitutional authority and accountability, controllable infrastructure, federated and inclusive capability, and legal memory.

Policy paper · Pakistan · Issue-I 2026

KSC.JUSNREM

Evolutionary, Strategic and Anticipatory Legal Intelligence