
Analytical working paper

Data Embassies and Saudi Sovereign Continuity: A Testable Comparative Framework

An analytical working paper comparing the legal protection of a data embassy, cases of record continuity under war and disaster, and cryptographic distribution, with proposed tests for any Saudi application.

Article date

October 18, 2026

Author

Safwan AlModhayan

Keywords: data embassy · sovereign continuity · digital sovereignty · threshold cryptography · continuity of government · risk management

An analytical working paper derived from the author's essay and open sources available through 18 October 2026. It is not peer-reviewed research, legal advice, or a report of a completed experiment or actual government results.

isafwan.com/en/research/data-embassies-sovereign-continuity/

Abstract

This paper examines Sovereign Continuity and the conditions under which foreign hosting of government data could support it, rather than amounting to a remote backup or a new dependency. It treats state continuity as a function of records, software, identity, signatures, communications, and legal authority. Data integrity alone does not establish usability or truth.

The paper uses documentary comparison. It reads the Estonia–Luxembourg agreement as a legal case and Ukraine, Kashmir, Syria, Sudan, and Svalbard as cases exposing different patterns of failure and recovery. It relates those cases to disaster recovery, Common-Mode Failure, secret sharing, record integrity, and Saudi controls for data transfer and cloud computing. ^{[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16]}

Its result is a test framework, not an experimental finding. A Saudi model should be evaluated by the independence of failure points; the ability to operate specified functions within a Recovery Time Objective (RTO) and Recovery Point Objective (RPO); lawful authorization; verifiable Provenance; regulatory compliance; and the capacity to change the host, supplier, and cryptographic algorithm. The paper does not claim that foreign hosting is necessary for every function or lawful for every data class.

Research Question and Scope

The principal question is: under what legal, technical, and operational conditions could a multi-site arrangement, partly outside the Kingdom, reduce the risk that Saudi Arabia loses the capacity to prove rights and operate selected sovereign functions when sites, networks, or administrative authorities fail?

Four subquestions follow. What does legal protection add beyond a hosting contract? What minimum must travel with the data for a function to remain operable? How can keys and copies be distributed without creating unilateral external authority? How should benefits and risks be tested before sensitive data is used?

The paper does not assess the legality of a particular project, which would require the data class, processing purpose, operating design, host states, and competent authorities to be known. It offers no quantitative estimate of war probability or forecast of financial effect, and it does not claim a causal relationship between data embassies and market stability.

Documentary Method and Case Selection

The analysis uses primary or near-event sources where possible: the official Estonia–Luxembourg agreement; government and judicial accounts from Ukraine and Kashmir; rights and humanitarian reporting on Syria and Sudan; documentation from the Svalbard

Global Seed Vault; Saudi regulations and controls; and original or normative material from Shamir and the National Institute of Standards and Technology (NIST). News reports and official statements are treated as bounded windows, not raised to independent verification when they are not.

Cases were selected for their analytical function, not because they are equivalent. Estonia supplies a legal hosting mechanism. Ukraine offers an official example of critical records surviving a strike on a backup site. Kashmir and Syria expose the effect of lost records on rights. Sudan separates data preservation from connectivity. Svalbard clarifies recovery of capacity rather than passive retention. ^{[1] [2] [3] [4] [5] [6] [7] [8] [9]}

The cases are compared on six dimensions: the protected asset, threat, site independence, capacity for recovery and operation, authority to order recovery, and limits of available evidence. This method does not permit statistical generalization. It identifies conditions that can be converted into hypotheses and tests for a pilot.

Operational Definitions

A Data Embassy is defined here as a foreign hosting site for government data and systems with a legal status created by agreement between two states. It does not imply a transfer of territory or automatic diplomatic immunity. Sovereign Continuity is a state's capacity to keep selected public functions operable and verifiable through severe disruption while retaining legal decision-making and ultimate control.

Disaster Recovery restores a technical resource after interruption. Continuity of Government sustains essential governing functions during interruption or restores them within acceptable limits. A technical recovery can therefore succeed while the public outcome fails if the system returns after the right or service has exhausted the time it can tolerate.

Provenance means tracing the origin of data, its modifications, and the authority for each change. Integrity means detecting unauthorized change; it does not prove that the initial entry was correct. Common-Mode Failure is the defeat of redundant arrangements by a shared cause, which makes genuine diversity more important than nominal geographic distribution. ^[10]

Comparison: Cases and Lessons

The Estonian case shows that legal value comes from the text rather than the name. The agreement defines inviolability, entry, communications, applicable law, dispute, termination, and delivery. It also states that the Vienna Convention is insufficient by itself. The site does not become Estonian territory; it receives bounded protection under an international agreement. ^[1]

Ukraine's official account suggests that distributing registers and preparing alternate resources before the danger fully materialized could stop physical damage from interrupting critical records. It remains an official account, not an independent audit of every system. Kashmir and Syria show how lost documents weaken proof even where the underlying legal claim theoretically survives. Sudan shows that a sound archive cannot provide a service when communications, identity, or payments are unavailable. ^{[3] [4] [5] [6] [7]}

Svalbard offers a functional measure. Preservation succeeded when samples were withdrawn, planted, multiplied, and deposited again. By analytical analogy, a ministry's copy is not a continuing capability until software can run, identity and signatures can be checked, and the record can be used through an authorized process. The analogy does not equate seed with data; it isolates a criterion of functional recovery. ^[8]

Legal Framework: Defined Protection, Not a Sovereign Vacuum

The Estonia–Luxembourg agreement protects the site against search, requisition, attachment, and execution, and requires consent from Estonia's representative for entry. Emergency consent is presumed only for immediate protection from a safety risk. Article 6 treats the data and systems as Estonian archives, protects official communications, and permits encryption. Article 8, however, preserves the application of international law, European Union law, and Luxembourg law where relevant, and provides for arbitration. ^[1]

Article 10 makes termination effective twenty-four months after notice. It distinguishes delivery to the authorized representative from the case in which that representative cannot be identified, when the assets remain protected and may be given only to a legal

representative. These clauses matter because they determine the archive's fate when relations or representation become contested instead of leaving that decision to a data-center operator. ^[1]

In Saudi Arabia, transfers of personal data outside the Kingdom are subject to national-security and vital-interest conditions, necessity, protection, individual rights, adequacy or safeguards, and specified derogations. An international agreement is one possible route within competent-authority procedures, not automatic approval. The Cloud Cybersecurity Controls are a security framework within their scope; they do not replace data-protection law, information classification, or sector requirements. ^{[14] [15]}

Technical Framework: Distributing Data and Authority

Three techniques must be separated. Authenticated Encryption protects confidentiality and detects tampering. Erasure Coding distributes fragments so content can survive loss. Threshold Cryptography distributes authority over keys or cryptographic operations. Treating one of these layers as though it performed all three jobs produces a system that is secure mainly in the presentation.

Shamir's Secret Sharing offers a threshold guarantee: under the correct mathematical implementation, a threshold group can reconstruct a secret and a smaller group learns nothing about it. A three-of-five example tolerates the loss of two shares. It does not prove data availability, lawful authorization, or security of the computers holding those shares. Custodians must be independent; shares require protection, rotation, and monitoring; and the replacement of an unavailable or untrusted custodian must be exercised. ^[11]

Multi-Party Computation and Threshold Signatures may allow operations without assembling the full key in one place, supported by Hardware Security Modules (HSMs). Protocol complexity, however, increases the burden of audit and incident response. The relevant test is whether the technique reduces a defined risk and remains operable under the institution's worst credible conditions.

Record Integrity, Event Truth, and Authority to Change

A Cryptographic Hash, Merkle Tree, or Tamper-Evident Log can show that a copy linked to a recorded fingerprint has not changed without detection. Documentation for Keyless Signature Infrastructure (KSI) describes verification of signing time, integrity, sequence, and an input fingerprint. Because the description comes from the provider, it is not treated as independent confirmation of every product claim. ^[12]

Evidence of integrity does not show that the original event was true, that the person entering it was authorized, or that a lawful amendment was not wrongly blocked. A design needs three related layers: input correctness supported by evidence and process; copy integrity supported by cryptography and logs; and authority to amend supported by identity, signature, and legal review.

Provenance becomes useful when it identifies the known-good version, the actor who changed it, the authority used, and the change that should be reversed. Its importance rises with data poisoning, impersonation, and automation capable of distributing a bad change quickly to every copy.

Authority in an Emergency

Technical capacity to recover should not be identical to legal authority to order recovery. The proposed model separates four roles: the lawful authority that decides; custodians who act only when the key-share threshold is met; the alternate-environment operator; and an independent auditor who checks the request, record, and result.

The model needs predefined emergency states, succession, objection channels, a policy for conflicting orders, and a decision record that no single party can erase. It also needs a way to authenticate the requester when the primary identity provider is unavailable. Exercises should include an absent official and divided communications between institutions.

Neither a foreign host nor a commercial supplier should settle a constitutional dispute. The interstate agreement, commercial contract, and technical protocol must define what a host may and may not do, how assets are protected when the representative cannot be identified, and how they move to another host.

Proposed Risk Matrix

The matrix describes risk along two axes: likelihood of the cause and impact on the sovereign function. Categories include physical, cyber, operational, legal, political, supplier, and internal-authority risk. Each entry records the affected asset, common failure point, preventive control, detective control, recovery path, and evidence required to close the test.

Scenarios include the loss of two sites; interruption of an international communications route; a sudden legal prohibition in a host state; failure of a shared management interface; theft of a key share; intentional but erroneous deletion distributed by synchronization; conflicting recovery requests; and inability to update a cryptographic algorithm. Some may have low probability and sufficiently high impact to justify a countermeasure or exercise.

The matrix should expose residual risk after controls rather than paint every cell green. It must distinguish loss of confidentiality, loss of availability, corruption of evidence, and the lawful credential used for an unlawful purpose. Treating one may worsen another: a higher threshold can resist capture while slowing recovery.

Testable Analytical Propositions

The first proposition is that geographic distribution reduces downtime only when it extends to operational dependencies, including identity, keys, administration, and communications. It can be tested by comparing recovery from geographically distributed but centrally managed sites with recovery using alternate identity and management paths while holding function and data as constant as practical.

The second proposition is that distributed key authority reduces unilateral capture risk but may increase recovery time and human procedural failure. Tests can vary the threshold, number of custodians, and absence of particular custodians, then measure authorization time, errors, and rejected requests. A three-of-five model is not assumed to be optimal; risk modeling and exercises should determine the result.

The third proposition is that a copy with verifiable Provenance reduces the time required to identify a sound version after tampering, provided trusted fingerprints and authority logs remain independent of the affected system. The fourth is that a Controlled Degraded

Mode restores useful public output faster than full-system recovery without exceeding rights constraints, if its functions are defined in advance and every use is reviewed.

These propositions contain no implied results. Tests may show that complexity erased the benefit, that a particular function cannot tolerate external hosting, or that an independent domestic path is cheaper and more stable. A pilot is valuable because it permits those answers before long-term dependence is built.

Economic Evaluation Framework

Evaluation should compare lifecycle cost with interruption cost, not a storage bill with no spending. Lifecycle cost includes creation, connectivity, testing, training, audit, contracts, key rotation, algorithm change, and supplier exit. Interruption cost includes lost transactions, manual work, delayed rights, restoration of trust, and effects on dependent institutions.

A baseline can be built from anonymized internal incidents and exercises, then used to measure restoration time, data loss, staff hours, and the cost of moving into alternate operation. A market movement or one wartime case should not become a fixed financial coefficient. The value of continuity depends on the function, outage duration, available substitutes, and expectations of affected parties.

Supplier and host-state lock-in must also be priced. What will migration cost if law or contract changes? How long will it take to extract data, keys, software, and logs in usable formats? A periodic exit test provides a better figure than an untested clause and reveals whether claimed diversity operates outside paper.

Testable Evaluation Criteria

The first criterion is functional. Each critical service needs a minimum output that a citizen or institution can use, rather than a server merely turning on. The time measures are the Recovery Time Objective (RTO), the maximum tolerable outage, and the Recovery Point Objective (RPO), the point to which the system can return and thus the acceptable data loss relative to the latest copy. ^[13]

The second criterion is independence. Recovery must work after the assumed number of sites or custodians has been lost, and after a shared supplier, identity provider, or communications path fails. Independence is measured by common dependencies discovered, not cities marked on a map. The third criterion is recovery integrity: a poisoned or unauthorized version must be rejected before service restarts, and Provenance for the chosen version must be demonstrated.

The fourth criterion is lawful authority: a request below the threshold or from an unauthorized body must fail, while succession must work when an official is absent. The fifth is exit: data, keys, software, and audit records must move to an alternate host within known time and cost. The sixth is compliance: classification, purpose, legal basis, minimization, and competent-authority decisions must be established before real data enters. These are proposed measures; the paper does not claim that an unperformed test has passed.

Phased Pilot Design

The first phase should use synthetic data and a non-sensitive service that resembles the dependency structure of a real government function. The team maps the chain, sets RTO and RPO, and builds encrypted preservation, an alternate environment, distributed key authority, and an audit record. Real personal data is unnecessary for proving a concept that can be tested without it.

The second phase runs compound-failure exercises under independent observation: lost sites, absent custodians, severed communications, a poisoned copy, an unauthorized request, and migration to a different supplier. It records time, decisions, human failures, and dependencies missing from the theoretical map. One successful restoration is not evidence of permanent readiness.

The pilot should not advance to more sensitive data or functions until independent legal, technical, and privacy review is complete, material defects are closed, and exit has been demonstrated. The result may be to exclude foreign hosting for a category. That is a sound result if testing produced it instead of a slogan predetermining the answer.

Implementation and Governance

Governance requires an owner of the function, not merely an owner of storage. The record-owning body understands the effect of loss; the digital body manages integration; the cybersecurity body tests defense and response; the regulator reviews transfer and privacy; and the foreign ministry negotiates legal status. Responsibility for accepting risk must be written rather than dispersed until it disappears.

Contracts need audit rights, incident notification, named processing locations and subcontractors, commitments to return assets and destroy copies, and transition assistance. Compliance should not depend on a report supplied solely by the vendor. An interstate agreement addresses entry, seizure, communications, law, dispute, termination, and representation.

Long-lived assets require Cryptographic Agility: an inventory of algorithms, certificates, and keys; separation from applications where practical; and plans for rotation and re-encryption. NIST's approval of Federal Information Processing Standards (FIPS) 203, 204, and 205 in August 2024 does not show that present cryptography has collapsed. It shows that algorithm migration is an operational event for which capacity should exist before necessity arrives. ^[16]

Limitations and Uncertainty

Several cases rely on government or journalistic accounts that do not expose complete operational records. Open sources do not reveal every detail of Ukraine's recovery capacity, the precise condition of every Sudanese document, or the effect of each outage on each service. The cases are therefore used only within what their sources establish, not as comprehensive audits.

Comparison among legal archives, seeds, and government systems is a limited functional analogy, not a claim of physical equivalence. Shamir's scheme provides a mathematical property under its assumptions; it does not prove implementation security or custodian independence. KSI materials describe a product from its provider and do not establish original truth or use across every Estonian service.

This paper contains no Saudi implementation cost, performance measurement, or compliance determination. Geopolitical and legal risks also change over time. Any execution decision would require current threat analysis, data classification, testing, contracts, agreements, and independent review.

Case selection is subject to availability bias. Events documented by governments, courts, or the media are easier to study than failures handled internally or kept secret. A reported success may conceal secondary services that failed; a documented failure may reflect greater transparency rather than worse performance. The paper does not use case counts to rank states or estimate a failure rate. It uses them to derive questions that a Saudi test environment can answer.

Conclusion

A data embassy is a possible instrument within a wider architecture; it is not the architecture itself. Agreements can provide legal protection that a commercial name cannot. Distribution can resist some failures if sites, administrations, and keys are genuinely independent. Yet data does not become a public function without software, identity, communications, signatures, and authority.

A defensible Saudi framework would be selective, function-led, and tested. It would define tolerable time and loss, separate authority from possession, include Provenance and lawful authorization in recovery, and place transfers under the applicable rules and competent authorities. Some functions may remain domestic; some may use protected foreign hosting; others may distribute keys or evidence rather than content.

Strategic value does not lie in the number of embassies or the volume stored. It lies in a demonstrable answer to one question: after losing sites, communications, and custodians, can the state still prove the correct right and operate the minimum service through a lawful decision, within the time society can bear?

Sovereign Continuity Gates

1	2	3	4
Recovery Time Objective (RTO) and Recovery Point Objective (RPO)	Legal and technical independence from Common-Mode Failure	Distributed Threshold Authorization	Tested recovery with verifiable Provenance

The pilot should not advance to real data until it passes all four gates: a defined function, reduced common dependency, valid authority, and proof of sound recovery within accepted time and loss.

References

1. [Agreement between Estonia and Luxembourg on the hosting of data and information systems](#)
Riigi Teataja, June 20, 2017
2. [The Legal Status of Data Embassies](#)
International and Comparative Law Quarterly, January 1, 2019
3. [Ukraine's cybersecurity infrastructure protected state registers during the war](#)
President of Ukraine, September 6, 2022
4. [Farooq Ahmad Dar v. State of Jammu and Kashmir](#)
High Court of Jammu and Kashmir and Ladakh, April 13, 2022
5. [Q&A: Syria's New Property Law](#)
Human Rights Watch, May 29, 2018
6. [30 million Sudanese historical documents at risk of deterioration](#)
Asharq Al-Awsat, June 26, 2026
7. [Sudan telecommunications joint statement](#)
Norwegian Refugee Council, May 3, 2024
8. [ICARDA seeds safe back in Lebanon and Morocco](#)
Svalbard Global Seed Vault, October 27, 2017
9. [Norges tilstedeværelse i Storbritannia under 2. verdenskrig](#)
National Archives of Norway
10. [Engineering Trustworthy Secure Systems](#)
NIST, March 1, 2022
11. [How to Share a Secret](#)
Communications of the ACM, November 1, 1979

12. KSI Technology
Guardtime
13. Contingency Planning Guide for Federal Information Systems
NIST, May 1, 2010
14. Implementing Regulations for Personal Data Transfer outside the Kingdom
SDAIA
15. Cloud Cybersecurity Controls CCC–2:2024
National Cybersecurity Authority
16. NIST Releases First 3 Finalized Post-Quantum Encryption Standards
NIST, August 13, 2024