16TH ITU ACADEMIC CONFERENCE

# ITU KALEIDOSCOPE
## GENEVA 2026

*AI and frontier technologies for good*

7-9 July 2026
Geneva, Switzerland

Hosted by AI for Good Global Summit

# Enforceable Digital Sovereignty In Government Cloud Procurement

9 July 2026

**Dickson Marfo Fosu**
Responsible Artificial Intelligence Lab – KNUST, Ghana

Session 7.6



ITU KALEIDOSCOPE
GENEVA 2026

# Background

## Why Government Cloud Procurement Is a Sovereignty Issue

**01** **Operational Constitutional Authority**

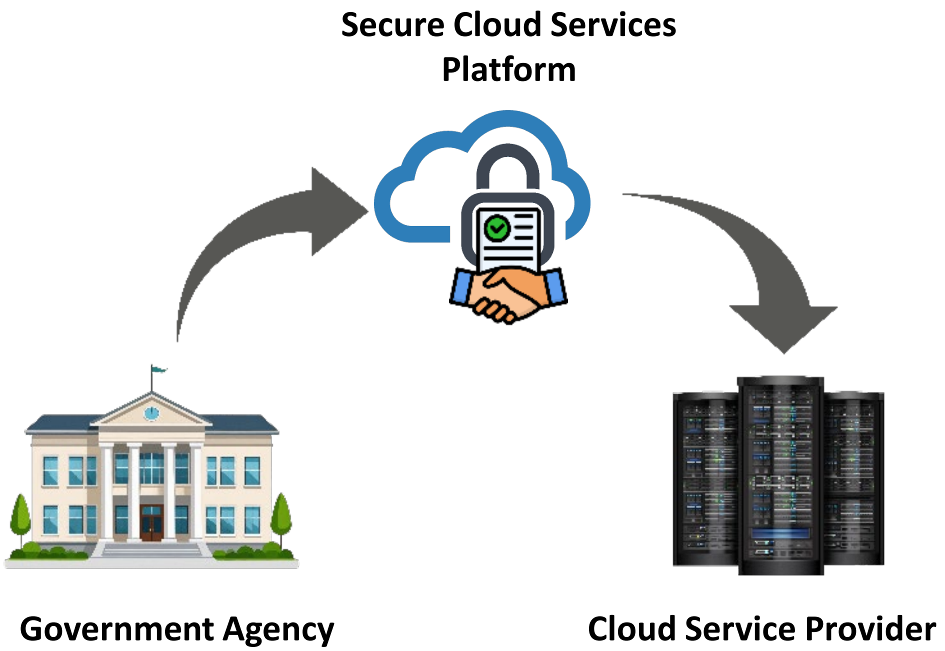
Control over critical digital assets in cloud contracts ensuring lawful data governance and national sovereignty.

**02** **National Security Safeguards**

Enforceable cloud procurement instruments mitigate exposure to extraterritorial compelled access and enhance cyber security.

**03** **Continuity of Government Services**

Contracts ensure resilience, observability, and transition support to maintain public administration during disruptions.



# The Central Problem

Residency ≠ *Sovereignty*

## ENFORCEABLE AGENCY

Sovereignty is a state's enforceable legal control over critical digital assets.

**The Residency Proxy:** Many assume storage within national borders equals control. This is false in modern cloud environments.

*"A system can be locally hosted and still be effectively captured by foreign jurisdiction."*

# The Technical Case

## Why Residency Fails

**01**

### Extraterritorial Compelled Access

US CLOUD Act and similar doctrines allow foreign access based on provider control, regardless of the physical location of the data.

**02**

### Control-Plane Externalization

Identity and key-management often reside outside national jurisdiction even when the data plane is local.

**03**

### Egress Economics

Punitive fees and technical timelines make practical data export infeasible at a national scale during exit.

# The Sovereignty Audit Lens

The lens makes existing ITU-T and ISO/IEC requirements enforceable through procurement design.

| PORTABILITY | OBSERVABILITY | REVERSIBILITY | LOCALITY | RESILIENCE |
|---|---|---|---|---|
| Feasibility of data and workload migration within economic and time constraints | Capacity to independently verify administrative actions and detect compromise | Executable contract termination and safe, structured data return | Jurisdictional and cryptographic anchoring of data and control functions | Persistence of sovereign control during infrastructure shocks and connectivity loss |
| **ISO/IEC 19941** | **ISO/IEC 27017**<br>**NIST SP 800-92** | **ISO/IEC 27036-4**<br>**SWIPO Codes of Conduct** | **ITU-T Y.3502**<br>**ISO/IEC 19790**<br>**ISO/IEC 19944-1** | **ITU-T Y.3513** |

# The Sovereignty Audit (A)

| THE TEST | THE RECOMMENDATION |
|---|---|

### Portability: The "Hostage" Test

- Calculate Total Cost of exiting provider.
- Check if data is in open formats.


Mandate transparent exit costs and data fees in contracts.

### Observability: The "Black Box" Test

- Check for a "Subpoena Notification Clause"
- Confirm auditability of access logs for actions

Require real-time audit logs and notifications for foreign data demands.

### Reversibility: The "Contract" Test

- Check if local authorities can terminate or suspend service without foreign approval

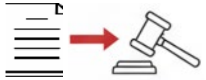

Enforce local law precedence over foreign legal orders in contracts.

# The Sovereignty Audit (B)

| THE TEST | THE RECOMMENDATION |
|---|---|

### Locality: The “Control” Test

- Check if the parent company is foreign
- Check if local law supersedes foreign orders.



Demand local jurisdiction for all data-related decisions.

### Resilience: The “Shock” Test

- Verify the "Kill Switch" Simulation
- Confirm disaster recovery sites are in trusted jurisdictions

Require verifiable off-ramp strategies and failover plans.

# Case Study

## Project Mbegu: The Physics of Egress

**111**

**Days to Export 1.2 PB**
at 1 Gbps continuous bandwidth

111 > 90

DAYS TO EXIT

DAYS ALLOWED

### ARCHITECTURAL CROSS-SECTION

| | |
|---|---|
| **Identity and authentication** | EXTERNALISED |
| **Key management and HSM** | PROVIDER-HELD |
| **Privileged admin plane** | FOREIGN DOMICILE |
| **Compute, storage, and data** | LOCAL REGION |

## Strategic Capture Analysis

If a contract has a **90-day retention window**, but technical export requires **111 days**, the state has effectively ceded autonomy.

**Exit Penalty:** $108,000 in egress fees alone (AWS 2026 pricing equivalent).

# Key Findings

## Strategic Capture Pattern

1. **Control Plane Isolation:** Administration from outside jurisdiction creates ultimate capture.
2. **Cryptographic Blindness:** Provider-held keys render local laws unenforceable.
3. **Identity Dependence:** Authentication relying on foreign services leaves systems ungovernable during shocks.
4. **Retention Gaps:** Egress economics must match contractual exit windows.

> “
>
> *Without a reversible exit path that fits within retention limits, the client has effectively ceded strategic autonomy to the provider.*
>
> **Cigref, 2025**

# The 7-Clause Procurement Schedule

**01**
**Ransom-free exit**
No punitive egress fees on termination. Neutralises economic capture.
PORTABILITY

**02**
**Transition bridge**
Guaranteed time and technical support for migration after termination.
PORTABILITY

**03**
**Sovereign key custody**
Hold Your Own Key (HYOK) or external key management outside provider control.
LOCALITY

**04**
**Notify-and-challenge covenant**
Provider acts as a legal shield against extraterritorial access where law permits.
OBSERVABILITY

**05**
**Island-mode guarantee**
Operational controllability survives connectivity disruptions.
RESILIENCE

**06**
**Immutable log shipping**
Telemetry to customer-controlled, out-of-band storage. Verifiable independently.
OBSERVABILITY

**07**
**Supply chain transparency**
SBOM disclosure and rapid vulnerability notifications.
REVERSIBILITY

# Implementation

## Verification Mechanisms

### PRE-AWARD
Proof before signature

1. Third-party HSM attestations verifying cryptographic module sovereignty
2. Log export configuration evidence and independent routing confirmation
3. Simulated island-mode continuity testing under real network isolation
4. Egress feasibility disclosure (time and cost) for full dataset

### POST-AWARD
Enforcement during contract

1. Annual sovereign audit rights exercised by the procuring agency
2. Mandatory breach and compelled-access notification obligations
3. SLA penalties triggered by egress barriers or lock-in mechanisms
4. Termination without exit penalties on documented non-compliance

# Conclusion

01 **Digital sovereignty is enforced through procurement controls, and not through data residency.**

02 **The Sovereignty Audit Lens converts abstract policy mandates into measurable, standards-grounded evidence artifacts.**

03 **The Seven-Clause Schedule converts that evidence into binding tender controls any government can adopt.**

# Thank you!