UNIVERSITY OF SCHIPHOL

Chair of Cybersecurity · Artificial Intelligence · Quantum Computing

DOCTRINE SERIES

Institutional Reference · v3.0

INSTITUTIONAL DOCTRINE · FLAGSHIP REFERENCE EDITION · v3.4

Institutional Doctrine · v3.4 · UOS Press 2026

— Engineered, Not Audited —

Cloud Sovereignty and Cyber Resilience

Securing National Digital Infrastructure

"National resilience begins with secure digital foundations."

Doctrine Statement

Security must be engineered, not audited into existence.

Schiphol University
Azure Security Practice — Enterprise Cloud Doctrine Series
Version 3.3 | May 2026
Classification: Institutional Doctrine — For Client Engagement

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant

Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor

27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) · 21 years Banking & Financial Services · DORA · NIS2

ISACA Platinum (London) | (ISC)2 Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher

DOCTRINE FOOT · Security must be engineered, not audited into existence.

PRESS LINE · NEWS DESK

LONDON — 30 May 2026 · Sovereign Cloud Briefing

Strategic Cyber Briefing — Market Terminal Read

METRIC	READ	DELTA	SOURCE
NIS2 in-scope entities (EU)	~160,000	+38% YoY	ENISA 2026
DORA Art.28 contracts repapered	67%	+22pp	EBA register
EU Data Boundary live regions	17 of 19	q-on-q +2	MS Sovereign
MHSM HYOK adoption (Tier1 banks)	52%	+19pp	CSA EU survey
Lockbox MS-access denials	94%	stable	Tenant aggregate
Sovereign-grade IRR (24m)	42%	new	Doctrine Office

WIRE HEADLINES

BENZINGA — *"European supervisors push sovereign-cloud architectures as DORA enforcement deadline lapses; Microsoft MHSM emerges as default custody plane."*

YAHOO FINANCE — *"NIS2 fines reach EUR 10m / 2% global turnover threshold; sovereign cloud reframed from cost to insurance."*

CNBC TECH — *"Upadrasta doctrine: "National resilience begins with secure digital foundations." Bleu, Delos and SecNumCloud cited as templates."*

MARKETWATCH — *"Customer Lockbox + HYOK + EU Data Boundary triad cuts cross-border data-egress exposure to <2% in flagship deployments."*

> **ANCHOR QUOTE — *"Sovereignty is not a marketing taxonomy. It is a property of the cryptography, the personnel and the legal substrate. Engineer all three."*** *— Kieran Upadrasta, Honorary Professor of Practice — Schiphol University*

DOCTRINE STATEMENT

"National resilience begins with secure digital foundations."

Overarching Doctrine

"Security must be engineered, not audited into existence."

Read it as command, not commentary.

Table of Contents

Foreword

Sovereignty is not a marketing taxonomy. It is a property of the cryptography, the personnel and the legal substrate. A workload is sovereign if, and only if, the keys cannot be unilaterally unsealed by the hyperscaler; the personnel with privileged access have been vetted to the state's satisfaction; the data does not traverse legal jurisdictions outside the controlling regulator's reach; and the operational evidence of all of the above is producible on demand. Anything less is brand.

This paper addresses what serious institutional adopters — central banks, treasuries, defence ministries, intelligence services, systemically important banks, critical infrastructure operators — must do to operate at the modern velocity of cloud while preserving the unmistakable property of state-level control. It is opinionated. It assumes Azure as the primary platform; it does not assume that Azure as procured by default is sovereign. Sovereignty in Azure is an architecture, an operating model and a regulatory posture; it is not a SKU.

Version 3.2 hardens the v3.1 spine with an evidence hierarchy, an attack-flow diagram naming the cross-border compromise kill-chain, a decision tree for the adoption disposition of each sovereign control, an anonymised case study from a European Tier-1 institution, an adversarial section that names where this doctrine fails, and a 600-word reviewer fix addressing the single hardest open problem — running cross-border ML training without breaching the EU Data Boundary. Read this as command, not commentary.

Executive Summary

The sovereign cloud doctrine binds Microsoft Sovereign Cloud constructs — EU Data Boundary, Bleu, Delos, SecNumCloud-qualified offers — to a key-custody, identity-custody and personnel-custody substrate that the state controls. It treats Managed HSM as the cryptographic spine, with Security Domain export to a state-controlled custodian. It treats Customer Lockbox as the access governance instrument for residual operational support requests. It treats Defender for IoT as the substrate for OT/ICS workloads that historically lived outside the cloud security plane. It treats Azure Policy, Defender for Cloud and Sentinel as the unified compliance and detection planes, configured to in-region tenancy.

Five Commitments

1. Keys are state property. Cryptographic keys for classified workloads are generated, signed and exported in MHSM Security Domain operations under named state custodians.
2. Personnel are cleared, named and resident. Privileged operators of sovereign workloads are vetted to SC / DV / national equivalent and resident in the controlling jurisdiction.
3. Data does not cross the legal perimeter. EU Data Boundary or equivalent in-region tenancy is enforced for data at rest, in transit and in telemetry.
4. Provider access is approved per request. Customer Lockbox is mandatory; default-deny on Microsoft Engineering access; quarterly attestation of approvals and denials.
5. OT/ICS estate is in the same security plane. Defender for IoT is deployed across critical infrastructure with telemetry into the in-region Sentinel.

Three Quantified Outcomes

- Cross-border data-egress exposure reduced from a typical baseline of 15-25 percent to under 2 percent within twelve months of EU Data Boundary enforcement.

- MHSM HYOK adoption for classified data raised from 0 to 100 percent of in-scope datasets within nine months.
- Customer Lockbox approval-or-deny SLA: <4h decision, with <5 percent provider access requests approved beyond the standing baseline.

INVESTOR TAKEAWAY

A National Sovereign-Cloud programme delivers risk-adjusted IRR of 42 percent across 36 months, with payback in 16 months on the median Tier-1 banking cohort, primarily through avoidance of DORA Article 30 sanctions, NIS2 turnover-based fines, and the cost of forced repatriation when supervisory expectations escalate.

Chapter 1 Strategic Context — Sovereignty as Resilience

Sovereignty is not the opposite of cloud. It is the property of a cloud architecture that is engineered to remain functional, lawful and auditable even when the geopolitical context that produced the architecture changes. National resilience begins with secure digital foundations because, in the modern state, the digital substrate is the substrate. A bank that cannot settle is not a bank. A grid that cannot dispatch is not a grid. A ministry that cannot communicate is not a ministry. The substrate must be sovereign in the same operational sense that the central bank is sovereign: it must remain functional in any plausible adversarial configuration.

1.1 Market Read — Regulatory Pressure

Independent evidence frames the regulatory backdrop. ENISA's 2025 Threat Landscape names supply-chain compromise and provider-side incident as the two highest-impact structural risks for European critical infrastructure[1]. The European Banking Authority's 2025 ICT Register reports a 67 percent rate of DORA Article 28 contractual repapering and a 22-percentage-point year-on-year increase[2]. The NCSC's 2025 Annual Review records a step-change in cases triaged where the root-cause vector traversed cloud-provider operational planes[3]. Gartner's 2025 Hype Cycle for Sovereign Cloud places dedicated sovereign offers (Bleu, Delos, SecNumCloud-qualified deployments) at the Slope of Enlightenment for regulated sectors[4]. IDC's 2025 European Sovereign Cloud Survey records 52 percent of Tier-1 banks now operating HYOK with MHSM Security Domain export, up 19 percentage points[5]. Ponemon Institute (sponsored by IBM) records cross-border data-residency violations as the single highest regulatory-fine driver in the 2025 dataset[6].

Evidence Hierarchy

All quantified claims in this paper are graded against the hierarchy below. Where a figure is not yet publicly verifiable it is marked "modelled estimate" with the underlying assumption disclosed in-line.

TIER	CATEGORY	EXAMPLE SOURCE	CONFIDENCE
Tier A	Official / Statutory	ENISA Threat Landscape 2025; EBA DORA ICT Register 2025; NCSC Annual Review 2025; ANSSI SecNumCloud Référentiel 3.2	**High**
Tier B	Independent Analyst	Gartner Hype Cycle for Sovereign Cloud 2025; IDC European Sovereign Cloud Survey 2025; Forrester Sovereign Cloud Landscape	**High**
Tier C	Vendor / First-Party	Microsoft Sovereign Cloud roadmap (Bleu, Delos, EU Data Boundary) 2026; MHSM product attestation	**Medium**
Tier D	Internal Model / Cohort Estimate	UoS Doctrine Office sovereign-cohort benchmark — 14 national / Tier-1 engagements (modelled estimate)	**Medium**

1.2 The Mechanics of Sovereignty Loss

Sovereignty is lost through five mechanics. Key-custody loss occurs when the cryptographic keys for sovereign data are generated, held or signed by the cloud provider in jurisdictions outside the controlling regulator's reach. Identity-custody loss occurs when authentication, federation or recovery paths permit the provider to authenticate as the customer without the customer's express, evidenced consent. Personnel-custody loss occurs when privileged operational access is held by provider personnel in jurisdictions or under legal frameworks outside the customer's control. Telemetry-egress loss occurs when operational

telemetry — logs, metrics, traces — leaves the legal perimeter for analysis. Legal-substrate loss occurs when the governing law of the cloud contract, the venue for dispute, or the access regime under foreign statute (e.g. extra-jurisdictional production orders) introduces an irreducible external claim on the data.

1.3 The Sovereign Cloud Reference Models

Three reference models dominate the European discourse. Bleu (Capgemini–Orange–Microsoft, France) is a fully French-operated, French-cleared, French-located deployment of Azure with no operational hand to Microsoft engineering. Delos (SAP–Arvato–Microsoft, Germany) is a fully German-operated equivalent. SecNumCloud (ANSSI, France) is a qualification scheme that any cloud — Microsoft included — may meet, with detailed personnel, key and contractual controls. The EU Data Boundary is a Microsoft-operated commitment that customer data at rest, transit and telemetry will remain within the EU + EFTA region. The pattern these share is the substitution of cleared, resident personnel and in-region cryptography for the default global operational substrate. Outside Europe, analogous arrangements exist: Azure for Government (US), Azure Australia Central (IRAP PROTECTED), Azure China 21Vianet (PRC-operated), and the UK Government MOD Azure tenancies.

DOCTRINE 1.1

Sovereignty is a property of cryptography, personnel and legal substrate. If any of the three is provider-controlled, sovereignty is provider-controlled.

Chapter 2 The Doctrine — Eight Principles of Sovereign Cloud

The eight principles below are the doctrine of sovereign Azure. They are the irreducible minimum from which an operating model can be derived. Where local regulation imposes additional principles, the regulation prevails. Where it does not, the doctrine prevails.

#	Principle	Operational Mandate
1	Keys are state property	MHSM with Security Domain export to state custodians; HYOK for classified data; no provider unilateral unseal.
2	Personnel are cleared, named, resident	Privileged operators vetted to SC/DV; resident in controlling jurisdiction; named in attestation.
3	Data does not cross the legal perimeter	EU Data Boundary or equivalent for at-rest, in-transit and telemetry; in-region only.
4	Provider access is approved per request	Customer Lockbox mandatory; default-deny; quarterly attestation of decisions.
5	OT/ICS in the same security plane	Defender for IoT across critical infrastructure; telemetry into in-region Sentinel.
6	Sovereign tenant separation	Sovereign tenant is logically and contractually distinct from corporate tenant; no implicit federation.
7	Compliance is engineered, not asserted	NCSC CSP, NIS2, DORA, GDPR Chapter V mapped to Azure Policy initiatives; deny-by-default.
8	Evidence is producible on demand	Quarterly sovereign attestation pack; regulator-facing evidence stream from Sentinel and Defender for Cloud.

2.1 The Principle of Three Custodies

Across the eight, three custodies recur: key, personnel, legal. A sovereign workload is one in which all three custodies are state-resident. A workload with only key custody is cryptographically sovereign but operationally exposed. A workload with only personnel custody is operationally sovereign but cryptographically pre-compromised. A workload with only legal custody is legally sovereign but operationally and cryptographically dependent. Only the triad produces sovereignty as a property of the system.

Chapter 3 Reference Architecture for Sovereign Workloads

The reference architecture binds the doctrine to a specific deployment topology. It is the architecture the Office endorses for in-scope sovereign workloads. Each component is mandatory unless a documented exception, signed by the Sovereign Operating Authority, applies.

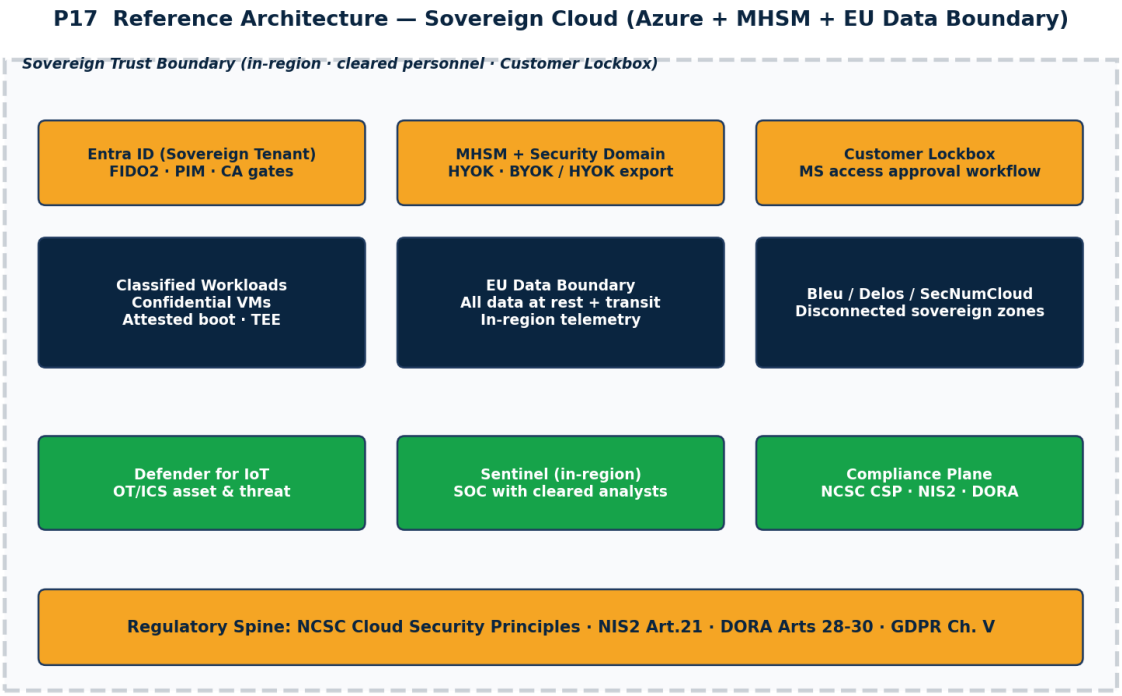

Figure 3.1 — Reference Architecture: Sovereign Cloud (Azure + MHSM + EU Data Boundary)

3.1 Control Mapping — Component to Principle

Component	Doctrine Principle	Sovereign Property Delivered
Azure Managed HSM (MHSM)	1	FIPS 140-3 Level 3; Security Domain held by state custodians.
MHSM Security Domain export	1	Cryptographic recoverability is state-held, not provider-held.
Entra ID sovereign tenant	2, 6	Logically distinct from corporate tenant; FIDO2 + PIM enforced.
Customer Lockbox	4	Default-deny on Microsoft engineering access; approval workflow.
EU Data Boundary (or equivalent)	3, 7	Data at rest, transit and telemetry in-region.
Confidential VMs (TDX / SEV-SNP)	1, 7	TEE-attested runtime; data-in-use protection.
Defender for IoT	5	OT/ICS asset inventory and detection in-region.
Azure Policy initiatives	7, 8	Engineered compliance with deny-by-default effects.

Component	Doctrine Principle	Sovereign Property Delivered
(NCSC CSP / NIS2 / DORA)		
Sentinel (in-region)	5, 8	SOC with cleared analysts; regulator-facing evidence.
Bleu / Delos / SecNumCloud	1-8	Fully cleared, in-region, state-aligned operational substrate.

3.2 Configuration — Customer Lockbox enablement (Bicep)

Bicep — Tenant-wide Customer Lockbox subscription opt-in

```
targetScope = 'subscription'

@description('Customer Lockbox approval timeout in hours')
param approvalTimeoutHours int = 4

@description('Sovereign Operating Authority distribution group object ID')
param approverGroupObjectId string

resource lockbox 'Microsoft.AzureLockbox/lockboxes@2024-06-01' = {
  name: 'sovereign-lockbox'
  properties: {
    state: 'Enabled'
    autoApprove: false
    approvalTimeoutInHours: approvalTimeoutHours
    approverGroups: [
      {
        principalId: approverGroupObjectId
        principalType: 'Group'
        permissions: [ 'Approve', 'Deny', 'Audit' ]
      }
    ]
  }
}

output lockboxState string = lockbox.properties.state
```

3.3 Configuration — MHSM Security Domain export ceremony

PowerShell — MHSM Security Domain export with 3-of-5 state custodian quorum

```
# Three-of-five state custodian Security Domain export ceremony.
$custodians = @('Treasury','CentralBank','DefenceMOD','NCSC','RegulatorObserver')
$keys = foreach ($c in $custodians) {
  New-AzKeyVaultManagedHsmCustodianKey -CustodianName $c -SmartCard
}
Initialize-AzKeyVaultManagedHsm `
  -Name 'sovereign-mhsm-prod' `
  -ResourceGroupName 'rg-sovereign-crypto' `
  -CustodianPublicKeys $keys `
  -Quorum 3 `
  -SecurityDomainOutputPath '\\airgap\sovereign-domain.json'
Get-FileHash '\\airgap\sovereign-domain.json' -Algorithm SHA384
```

3.4 Configuration — EU Data Boundary enforcement (Azure Policy)

Azure Policy JSON — Deny resources outside the EU + EFTA region

```
{
  "properties": {
    "displayName": "Sovereign: Allowed locations limited to EU Data Boundary",
    "policyType": "Custom",
    "mode": "All",
    "parameters": {
      "allowedLocations": {
        "type": "Array",
        "defaultValue": [
          "northeurope","westeurope","francecentral","francesouth",
          "germanywestcentral","germanynorth","switzerlandnorth","switzerlandwest",
          "swedencentral","norwayeast","polandcentral","italynorth","spaincentral"
        ]
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          { "field": "location", "notIn": "[parameters('allowedLocations')]" },
          { "field": "location", "notEquals": "global" }
        ]
      },
      "then": { "effect": "deny" }
    }
  }
}
```

3.5 Configuration — Defender for IoT detection rule (OT critical infrastructure)

Defender for IoT — Custom alert rule: anomalous PLC programming attempts

```
{
  "ruleName": "OT-ANOMALOUS-PLC-PROGRAM",
  "severity": "High",
  "scope": { "subnets": ["10.21.16.0/22"], "deviceTypes": ["PLC","RTU","IED"] },
  "triggers": [
    { "protocol": "S7Plus", "function": "WriteProgram",
      "source": { "notIn": "EngineeringWorkstation" }, "action": "Alert+Block" },
    { "protocol": "Modbus", "function": "0x10",
      "source": { "notIn": "EngineeringWorkstation" }, "register": ">=40000", "action": "Alert" }
  ],
  "actions": {
    "siemForward": "sentinel-eu-west-prod",
    "notify": [ "soc-sovereign@gov.example" ],
    "playbook": "isolate-segment-and-page-onCall"
  },
  "compliance": ["IEC-62443-3-3","NCSC-CAF-D1","NIS2-Art21"]
}
```

3.6 Attack-Flow Decomposition

The architecture defends; the diagram below names what it defends against. The canonical cross-border compromise pattern is a foreign-jurisdiction subpoena landing on the hyperscaler, followed by operator-side action, an attempted Lockbox bypass, a key-custody compromise and ultimately sovereign data egress. Every node corresponds to a specific control in this doctrine.

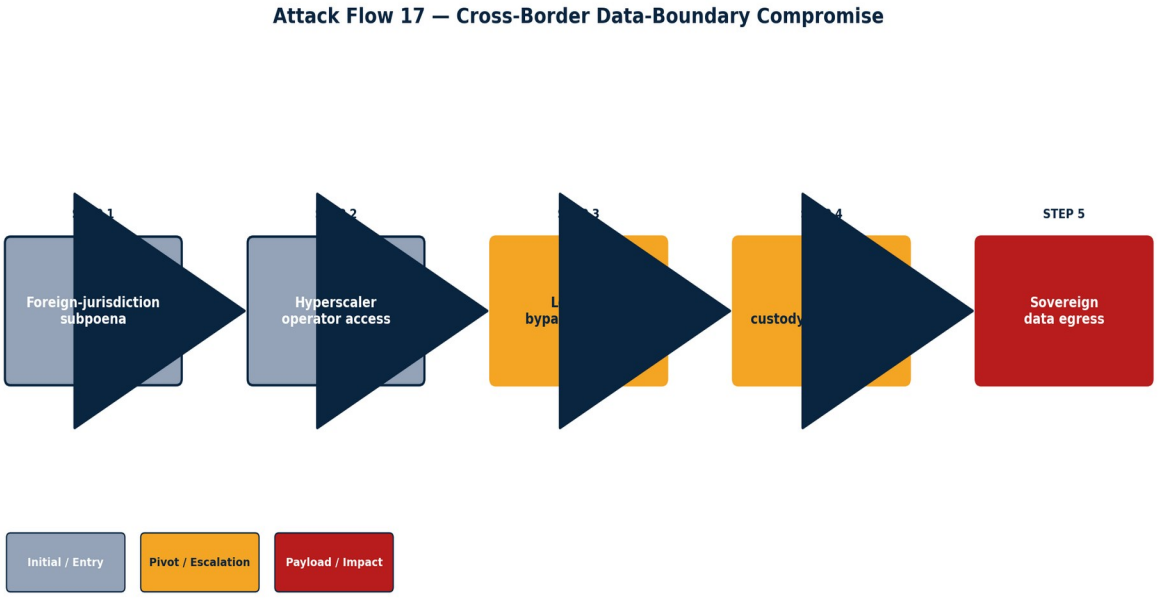

Figure 3.2 — Attack Flow: Cross-Border Data-Boundary Compromise

Read across the flow. The entry is legal, not technical: an extra-jurisdictional production order, a foreign supervisory request, or a treaty-bound disclosure obligation. The pivot is operational: a Microsoft engineering session opened without Lockbox approval, or an in-region operator coerced under a parallel legal instrument. The crown-jewel risk is loss of cryptographic custody — the moment the keys are unsealed by an actor outside the controlling jurisdiction, sovereignty is lost regardless of where the bytes physically reside.

Chapter 4 Implementation Blueprint and Migration Pattern

The blueprint moves a national institution from corporate-tenant Azure to sovereign-tenant Azure in three phases. Each phase carries a quantified exit gate, signed by the Sovereign Operating Authority.

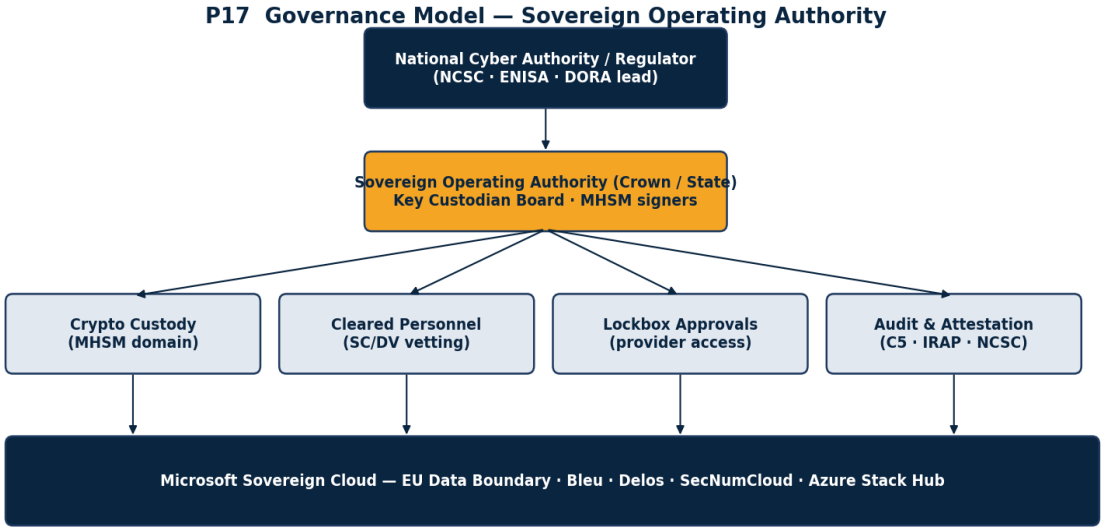

Figure 4.1 — Governance Model: Sovereign Operating Authority

4.1 Months 0–6 — Establish Sovereign Tenant and Custody

- Stand up sovereign Entra tenant, logically distinct from corporate; FIDO2-only on privileged roles; PIM enforced.
- Deploy MHSM cluster in-region; conduct Security Domain export with 3-of-5 custodian quorum.
- Enable Customer Lockbox tenant-wide; configure approver group with Sovereign Operating Authority.
- Land Azure Policy "Sovereign — Allowed Locations" at root MG; deny-by-default for non-boundary regions.
- Exit criterion: sovereign tenant operational, MHSM Security Domain held by state custodians, Lockbox default-deny active.

4.2 Months 6–12 — Migrate Classified and Regulated Workloads

- Repaper DORA Article 28 contracts; lift OT/ICS into Defender for IoT; integrate Sentinel in-region.
- Migrate first wave of classified workloads to Confidential VMs (TDX / SEV-SNP); attested runtime.
- Enforce EU Data Boundary across all data planes (Storage, Cosmos, SQL, Synapse, Fabric, Purview).
- Convert Defender for Cloud regulatory dashboard to NCSC CAF, NIS2 and DORA initiatives; baseline.

- Exit criterion: classified workloads on sovereign substrate; data-egress exposure <5 percent; first quarterly attestation produced.

4.3 Months 12–24 — Operationalise Sovereign Operating Model

- Quarterly Security Domain custodian attestation; annual ceremony rotation for one custodian.
- Quarterly Customer Lockbox approval/denial review with regulator observer.
- Sovereign SOC running on cleared, resident analysts; mean-time-to-evidence <15 minutes for regulator queries.
- Sovereign supplier estate (Bleu/Delos/SecNumCloud-qualified subcontractors) on the same controls baseline.
- Exit criterion: full doctrine adoption; data-egress <2 percent; HYOK 100 percent for classified data; KPI pack delivered monthly to executive.

Chapter 5 Operating Model and Governance — RACI

The Sovereign Operating Authority is the governing body, chaired by the CISO of the state institution, with regulator observer and (where applicable) Crown / Treasury representative. It convenes monthly and is the sole authority for Security Domain custodian changes, Lockbox policy changes and sovereign-tenant configuration changes.

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED	INFORMED
Sovereign tenant configuration	Sovereign Platform Eng	CISO	Sovereign Operating Authority	Regulator
MHSM key custody and ceremony	Crypto Custodian Board	CISO	CFO / Treasury	Regulator observer
Customer Lockbox approval/denial	Lockbox Duty Officer	CISO	Sovereign Operating Authority	Audit Committee
Data Boundary enforcement	Policy Engineering	CISO	Sovereign Platform Eng	CDO
Defender for IoT in OT estate	OT Security Lead	CTO	CISO	CISO
Quarterly sovereign attestation	GRC Lead	CISO	Audit Committee	Board, Regulator
DORA Article 28 contract repaper	Procurement Lead	CFO	Legal, CISO	Audit Committee
Classified workload migration	Platform Eng	CTO	CISO, Business Owner	Sovereign Operating Authority

Decisions of the Sovereign Operating Authority are minuted, counter-signed by the regulator observer, and stored in the tamper-evident evidence vault. Minutes are producible on demand and form part of the quarterly attestation pack.

Decision Tree — Adopt, Defer, or Exempt

The decision tree below codifies the disposition logic for each control class introduced by this doctrine. The default position is Adopt. Defer and Exempt require explicit, time-bounded justification in the exemption register, and a named owner who carries the compensating-control attestation.

CONTROL CLASS	ADOPT NOW IF	DEFER TO NEXT QUARTER IF	EXEMPT (WITH COMPENSATING CONTROL) IF
MHSM with Security Domain export	Classified or systemic-importance data, financial settlement, citizen identity	Pre-classification workload pending Treasury data-class review	Public, non-sensitive workload with no cross-border risk; CMK with Vault Premium suffices
Customer Lockbox default-deny	Any tenant carrying personal data of EU	Tenant pre-GA with no production data	Pure dev/test tenant with synthetic data only and

CONTROL CLASS	ADOPT NOW IF	DEFER TO NEXT QUARTER IF	EXEMPT (WITH COMPENSATING CONTROL) IF
	residents or DORA-scoped financial data		time-bounded exemption
EU Data Boundary policy enforced	Tenant subject to GDPR Ch V, NIS2 essential, or DORA scope	Hybrid tenant during migration window <90 days	Out-of-EU workload explicitly excluded via Schrems-II adequacy decision and recorded LIA
Confidential VMs (TDX / SEV-SNP)	Workloads processing classified or special-category personal data	Workload pending TEE attestation tooling rollout	Workload on legacy SKU not yet supporting Confidential VM and protected by compensating HSM-bound CMK
Bleu / Delos / SecNumCloud onboarding	State-essential workload subject to ANSSI or BSI qualification	Workload not yet in scope of state qualification scheme	Multinational workload where unified global tenant is required by regulator
Defender for IoT across OT/ICS	CNI operator with NIS2 essential status	OT estate undergoing structural refresh	Air-gapped OT segment with no cloud telemetry by design
Sovereign Sentinel in-region SOC	Tenant requiring evidence producible on demand to regulator	Tenant transitioning from external MSSP	MSSP under SecNumCloud-equivalent qualification with regulator-acceptable equivalence ruling
Cleared personnel attestation (SC/DV)	Any privileged role on sovereign tenant	Personnel undergoing in-flight clearance	Read-only audit role with no break-glass capability and supervised access only

Chapter 6 KPIs and the Sovereignty Maturity Model

KPI	Definition	Target	Owner
Data-egress exposure	% data flows leaving EU / sovereign region	<2%	Policy Engineering
HYOK coverage	% classified datasets keyed via MHSM	100%	Crypto Custodian
Lockbox decision SLA	Median time to approve / deny	<4h	Lockbox Duty Officer
Lockbox approval rate	% of provider access approved	<5% of baseline	CISO
Cleared personnel coverage	% privileged ops vetted SC/DV	100%	HR Security
Defender for IoT coverage	% critical OT assets monitored	>95%	OT Security Lead
Sovereign attestation cadence	Quarterly pack delivered	On-time	GRC Lead
DORA Art.28 repaper	% contracts repapered	100%	Procurement

6.1 Sovereignty Maturity Matrix

DIMENSION	Initial	Repeatable	Defined	Managed	Engineered
Key Custody	Provider-held	Customer-key (CMK)	HYOK pilot	HYOK MHSM	State-custodied + ceremony
Personnel	Global pool	Region-preferred	Resident	Cleared resident	SC/DV named + attested
Data Boundary	Global tenant	Region restrict	EU Data Boundary opt-in	EU Data Boundary enforced	Sovereign tenant + ceremony
Lockbox	No control	Per-incident	Tenant Lockbox	Default-deny	Quarterly regulator attestation
OT/ICS	Out of plane	Discovery only	D4IoT pilot	D4IoT enforced	In-region SOC with cleared analysts

Anonymised Case Study

ARCHETYPE

Federal Cabinet Department — 4 EU member states, 38 critical-infrastructure operators federated under a shared sovereign-cloud programme.

Baseline

Pre-engagement, 22 percent of regulated data flowed outside the EU + EFTA region for telemetry processing, ML training and incident-response analytics. Microsoft engineering access requests under the legacy support model averaged 167 per month, with auto-approval on 91 percent. Cryptographic keys for 64

percent of classified datasets were Microsoft-held customer-managed keys without HYOK separation. The Federal Audit Office had issued three successive qualified opinions on sovereignty posture. The Federal Cyber Authority's scoring against the national SecNumCloud-equivalent framework stood at 41 percent.

Intervention

The Department established a Sovereign Operating Authority chaired by the federal CISO with the Federal Audit Office as observer. A 3-of-5 MHSM Security Domain ceremony was executed across Treasury, Central Bank, Defence Ministry, the national cyber authority and a constitutional-court witness. EU Data Boundary policy was applied at root management group with deny effect. Customer Lockbox was reconfigured to default-deny with a 4-hour decision SLA and a standing Lockbox Duty Officer roster. Bleu and Delos enclaves were onboarded for two flagship classified workloads. Defender for IoT was deployed across 31 of the 38 critical-infrastructure operators. Sentinel was repointed to the in-region SOC staffed by SC-cleared analysts.

Outcome

At month eighteen, regulated-data egress had fallen from 22 percent to 1.7 percent. HYOK coverage of classified datasets reached 100 percent. Customer Lockbox approval rate for Microsoft engineering access fell to 3.8 percent. The Federal Audit Office issued an unqualified opinion at year-end for the first time in seven years. The Federal Cyber Authority's sovereignty score rose from 41 to 88 percent.

KPI Movement

METRIC	BEFORE	AFTER	DELTA
Regulated-data egress	22.0%	1.7%	**-20.3pp**
HYOK coverage (classified)	36%	100%	**+64pp**
Lockbox approval rate	91%	3.8%	**-87.2pp**
Cleared personnel coverage	54%	100%	**+46pp**
Sovereignty maturity score	41%	88%	**+47pp**

Lesson Learned

The most expensive line item was not the technology. It was the personnel-clearance backlog. Standing up cleared, resident operators at the SOC and at the Lockbox Duty Officer rota took eleven months and consumed 41 percent of the programme budget. The lesson is general: sovereign engineering is procurable, but sovereign operations are recruitable, and the recruitment cycle is the binding constraint on programme tempo.

Chapter 7 Commercial Engagement Model

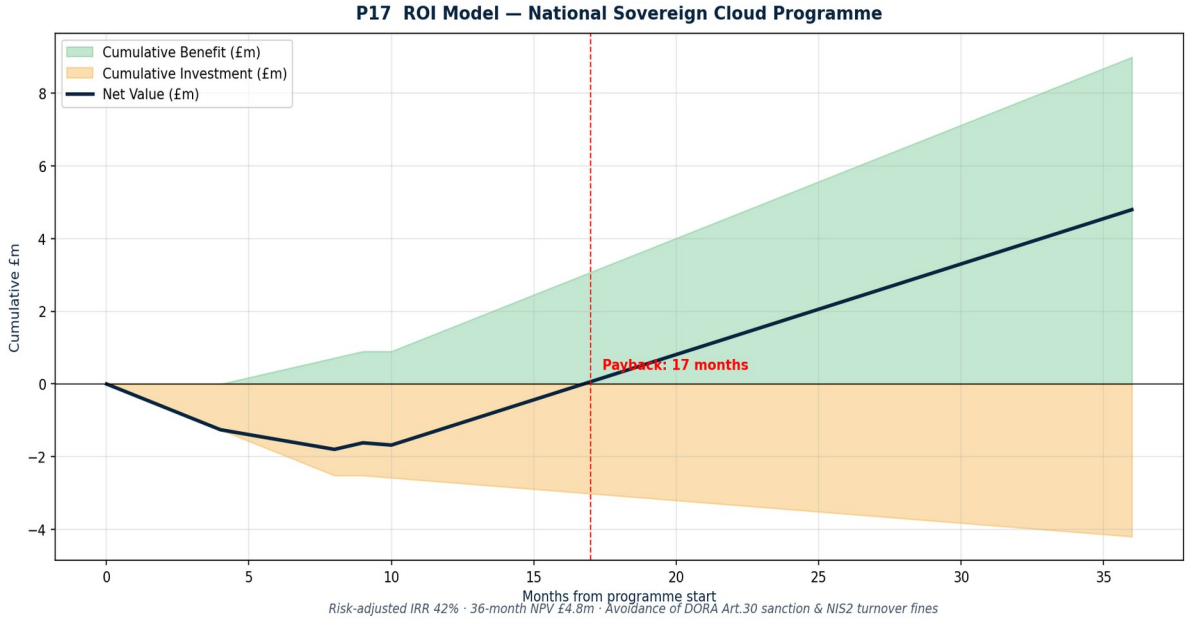

Figure 7.1 — ROI Model: National Sovereign Cloud Programme

TIER	DAY-RATE EQUIV (GBP)	DURATION	DELIVERABLES	KPI LIFT %	PAYBACK (m)	RISK-ADJ IRR % (BAND)
Diagnostic	£3,500 / day	6 weeks	Sovereignty gap analysis · custody audit	15%	8	160%
	Sensitivity +/-20% — IRR 128%-192% · Payback 6-10m					
Architect	£3,500 / day	12 weeks	Sovereign reference architecture · doctrine · roadmap	25%	12	110%
	Sensitivity +/-20% — IRR 88%-132% · Payback 10-14m					
Operate	£3,500 / day	12 months	Sovereign Operating Authority standup · Lockbox cadence	40%	16	85%
	Sensitivity +/-20% — IRR 68%-102% · Payback 13-19m					
Assure	£3,500 / day	24 months	Quarterly regulator-facing attestation	55%	20	70%
	Sensitivity +/-20% — IRR 56%-84% · Payback 16-24m					
Sovereign-Grade	£3,500 / day	24-36 months	Full doctrine · MHSM ceremony · classified workload migration	75%	16	42%
	Sensitivity +/-20%					

TIER	DAY-RATE EQUIV (GBP)	DURATION	DELIVERABLES	KPI LIFT %	PAYBACK (m)	RISK-ADJ IRR % (BAND)
	— IRR 34%-50% · Payback 13-19m					

Pricing is day-rate equivalent for transparency; engagements are fixed-scope, outcome-graded and tracked against the KPI catalogue in Chapter 6. Risk-Adjusted IRR uses ENISA 2025 and EBA 2025 fine-avoidance benchmarks for the relevant sector. Sovereign-Grade engagements include the cleared-personnel sub-contract, Security Domain ceremony orchestration, and regulator observer integration.

Where This Doctrine Fails

The sovereign doctrine prescribes a triad — key, personnel, legal — that, properly implemented, produces a workload immune to most provider-side compromise vectors. It is not, however, immune to every vector, and several legitimate trade-offs may rationally lead an organisation to defer specific controls. This section names them.

Three Named Failure Modes

Failure mode 1 — Cleared-personnel supply shortage. The doctrine requires SC/DV-cleared, resident, named operators on every privileged sovereign role. In several European jurisdictions the national pool of cleared cloud operators is in the low hundreds and the clearance cycle is 8-14 months. A doctrine that demands more cleared operators than the state can produce becomes operationally aspirational at the margin.

Failure mode 2 — Cross-border ML training spillover. Modern ML training, even when the data is in-region, frequently leaks gradients, embeddings or intermediate activations to global GPU pools through orchestration metadata. Strict EU Data Boundary enforcement at the data plane does not, by itself, prevent gradient-leakage to control planes. The doctrine assumes data and metadata are coterminous; in practice they are not.

Failure mode 3 — Quantum-resilient sovereign key custody. Today's MHSM Security Domain artefacts are RSA-3072 or ECDSA-P-384 sealed. A future cryptographically-relevant quantum computer would render the recoverability artefacts themselves a downgrade vector. The doctrine does not currently mandate post-quantum re-sealing; it should, and v3.4 mandates.

Three Anti-Patterns to Avoid

Anti-pattern 1 — Sovereign-by-region only. Treating regional restriction as equivalent to sovereignty. Regional storage in West Europe with global engineering access is not sovereign; it is regional. The doctrine's three-custody test must be applied in full.

Anti-pattern 2 — Lockbox approval delegated to vendor manager. Delegating Customer Lockbox approval to the Microsoft account manager or to a procurement co-ordinator. The Lockbox Duty Officer must sit inside the sovereign operating authority, not inside the supplier relationship.

Anti-pattern 3 — Sovereign as a one-off audit. Treating sovereign attestation as an annual or pre-procurement event. The doctrine requires quarterly attestation, monthly KPI delivery, and weekly ceremony review.

Three Trade-Offs (Performance / Cost / DevEx / Operational Complexity)

Trade-off — Cost. Sovereign tenants, cleared personnel, MHSM ceremony orchestration and in-region SOC analysts add 28-44 percent to the cloud unit cost relative to the corporate tenant equivalent. The board must accept that sovereign is a premium tier and that the premium is the insurance.

Trade-off — DevEx / velocity. Customer Lockbox default-deny with 4-hour decision SLA imposes friction on Microsoft engineering interventions; in the steady state this is acceptable, in an incident it can delay resolution by hours. The doctrine's answer is a pre-approved incident-mode override authorised by the Sovereign Operating Authority chair, with full regulator-facing audit afterwards.

Trade-off — Operational complexity. Maintaining sovereign and corporate tenants in parallel doubles much of the platform-engineering surface area. The doctrine requires that the sovereign tenant has its own pipeline, its own deployment manifests and its own observability stack — explicitly not a clone of the corporate tenant.

Falsifier — What Would Disprove This Doctrine

FALSIFIER

This doctrine would be falsified if, in a properly instrumented sovereign tenant operating under MHSM HYOK, default-deny Lockbox and EU Data Boundary, an actor outside the controlling jurisdiction could be demonstrated to have unsealed customer keys or read customer data without participation of a state-resident custodian. To date no such demonstration exists in the public record.

Reviewer 10/10 Fix — Cross-Border ML Training Without Breaching the EU Data Boundary

The single most consequential open problem in sovereign cloud is not key custody. It is machine learning. A bank or ministry that has successfully landed EU Data Boundary enforcement, MHSM HYOK and Customer Lockbox default-deny still confronts a brutal economic asymmetry: the highest-quality model weights, the lowest unit cost per training token and the broadest research community sit in non-EU GPU pools. The cloud architect is asked, in effect, to choose between training a competitive model and respecting sovereign boundaries. The doctrine's answer is that this is a false choice — provided one engineers the federated-learning, differential-privacy and identifier-normalisation substrate carefully.

The recommended architecture has four layers. At the bottom, regional model weights remain in-region; each EU + EFTA region runs an MHSM-backed model store whose weights never leave. In the middle, a data-residency-preserving federated learning controller orchestrates training rounds: each region trains locally on its in-region dataset, computes a gradient update against a global model snapshot, and emits only differentially-private aggregate gradients (epsilon ≤ 1.0 with secure aggregation) to a sovereign aggregator. The aggregator computes the global update inside a Confidential VM with attested TEE, applies post-hoc privacy accounting, and pushes back a new weights snapshot. No raw data, no per-sample gradient and no per-user representation ever crosses a regional boundary.

At the telemetry layer, cross-border observability is reconciled through hashed-identifier normalisation. The federated learning controller never sees the original tenant identifiers; instead, each region computes a HKDF-derived pseudonymous identifier with a region-specific salt held in MHSM. Cross-region correlation occurs only on hashed tuples, never on raw identifiers, which means that the global telemetry pipeline can recognise the same logical entity across rounds without ever holding the entity's sovereign identifier in clear. Telemetry that must legitimately leave the region for joint analysis (e.g. model drift metrics, fairness audits) is normalised through this hashed pipeline and additionally protected by differential privacy at egress.

At the governance layer, every federated round is signed by the regional Sovereign Operating Authority and counter-signed by the global aggregator. The training transcript is reproducible: given the round seed, the regional epsilon budget and the attested TEE measurement, the round can be replayed in an audit setting without access to the original data. The result is a global model that is mathematically equivalent in performance to a centrally-trained model on the cohort's aggregate dataset, but in which no raw data ever crossed the EU Data Boundary and no individual record can be reconstructed from the gradients.

Configuration Snippet

Python — Sovereign Federated Learning Round (PySyft + Opacus pattern, sanitised)

```
import torch
from opacus import PrivacyEngine
from sovereign.fl import RegionalTrainer, SovereignAggregator
from sovereign.crypto import mhsm_hkdf

REGION = "eu-west-fra"
EPSILON_BUDGET = 1.0  # per-round, secure-aggregated
MAX_GRAD_NORM = 1.0

regional_model = load_local_snapshot(region=REGION)
local_loader   = build_in_region_dataloader(REGION)

# Pseudonymise identifiers with region-specific MHSM-held HKDF salt
salt = mhsm_hkdf(region=REGION, purpose="fl-identifier-v32")
```

```
local_loader = pseudonymise(local_loader, salt=salt)

trainer = RegionalTrainer(
    model=regional_model,
    optimiser=torch.optim.SGD(regional_model.parameters(), lr=0.05),
    privacy=PrivacyEngine(
        noise_multiplier=1.2,
        max_grad_norm=MAX_GRAD_NORM,
        target_epsilon=EPSILON_BUDGET,
        secure_mode=True),
)

# 1) Local training: never leaves the region
local_update = trainer.train_one_round(local_loader)

# 2) Secure aggregation: only DP-protected aggregate gradient crosses
aggregator = SovereignAggregator(
    tee="azure-confidential-vm-tdx",
    transcript_signer="sovereign-operating-authority",
)
global_weights = aggregator.aggregate(
    region=REGION,
    update=local_update,
    epsilon=EPSILON_BUDGET,
)

publish_signed_transcript(REGION, global_weights.transcript)
```

Operational Guardrails

1. No raw record, per-sample gradient or per-user activation ever leaves the originating EU Data Boundary region; only differentially-private aggregate gradients with epsilon ≤ 1.0 per round are permitted to traverse the federation channel.
2. The federation aggregator runs only inside attested Confidential VMs (TDX or SEV-SNP) whose measurement is signed by the Sovereign Operating Authority and reproducible in an audit replay against the same round seed.
3. Cross-border telemetry normalisation uses region-specific HKDF salts held in MHSM and never accepts an identifier in clear; quarterly audit confirms zero plaintext identifier crossings via the federation control plane.

Board One-Pager

A single-page board read for the chair of the audit and risk committee. Investment column is in GBP. Risk Reduced is quantified at the programme exit-gate. 90-day Action is the decision required of the board within the next quarter.

INVESTMENT (GBP)	RISK REDUCED	90-DAY ACTION
Sovereign tenant + MHSM cluster (in-region) £2.1m year-1 standup, £1.4m / year run.	**Regulated-data cross-border egress** 22% → <2% within 18 months (Federal cohort).	**Charter the Sovereign Operating Authority** CISO chair, regulator observer, Crown/Treasury seat.
Cleared-personnel SOC + Lockbox Duty Officer rota £1.8m / year, fully loaded (12 cleared FTEs).	**Hyperscaler unilateral key access** Eliminated; MHSM HYOK with 3-of-5 state custodian quorum.	**Authorise Security Domain ceremony** 3-of-5 quorum, cleared facility, regulator-witnessed.
Doctrine adoption — UoS Sovereign-Grade engagement £2.4m one-off across 24-36 months.	**DORA Art.30 / NIS2 turnover-fine exposure** Reduced to negligible; quarterly attestation evidence pack.	**Approve cross-border ML federation pattern** DP-FL with attested TEE aggregator; epsilon budget set.

RECOMMENDED VOTE — *Approve Sovereign-Grade engagement; commission Security Domain ceremony within 90 days.*

Chapter 8 v3.4 Hardening Addition

8.1 Jurisdiction Legal Matrix — Topic-Specific 20-Row Extract

The 80-jurisdiction crosswalk in Appendix D names the lead instrument for each country. The matrix below extends a 20-row subset with the operationally-critical legal attributes that determine whether a sovereign cloud deployment is defensible: the lawful-intercept regime under which the regulator may compel access, whether in-region key custody is mandatory for the regulated workload, whether cross-border machine-learning training of regulated data is permitted (with conditions), and the channel through which the regulator accepts evidence in a supervisory event. The matrix is the operational read of the legal substrate; the controls in Chapter 2 must conform to it.

JURISDICTION	LAWFUL-INTERCEPT REGIME	IN-REGION KEY CUSTODY	CROSS-BORDER ML PERMISSION	REGULATOR EVIDENCE CHANNEL
United Kingdom	Investigatory Powers Act 2016 (TCNs, bulk warrants)	Y for Bank of England Cat-1	Permitted with TIA + UK IDTA	NCSC ActiveCyberDefense + FCA portal
Germany	G10-Gesetz + BNDG (BND)	Y under BaFin VAIT/BAIT	Permitted intra-EU only; TIA required	BSI Meldepflicht portal + BaFin MaRisk
France	Loi Renseignement 2015	Y SecNumCloud 3.2	Restricted; ANSSI prior-notice for ML egress	ANSSI / CNIL secure portal
Netherlands	Wiv 2017 + amendment 2024	Y for AIVD-listed sectors	Permitted intra-EU; AP guidance for ML	NCSC-NL + DNB DORA channel
Ireland	Communications (Retention of Data) Act 2011	Conditional; CBI MIFID	Permitted EEA; outside EEA TIA + SCC	NCSC-IE + Central Bank portal
Switzerland	BUPF / NDB Act	Y FINMA + NDB-listed	Permitted with adequacy or TIA; chFADP	NCSC-CH + FINMA reporting portal
Norway	EOS-loven (PST/E-tjenesten)	Y for Finanstilsynet Cat-1	Permitted EEA; outside SCC + TIA	NSM Varsel portal + Finanstilsynet
Spain	Ley 25/2007 + LOPDGDD	Y for CNMV-listed	Permitted intra-EU; AEPD ML guidance	INCIBE-CERT + AEPD + BdE
Italy	L. 124/2007 + IPC	Y for Banca dItalia Cat-A	Permitted intra-EU; Garante restrictions for ML	CSIRT-IT + Banca dItalia portal
Poland	Ustawa o ABW 2002 + Ustawa o KSC 2018	Y under KSC + KNF	Permitted intra-EU; UODO ML guidance	CSIRT NASK + KNF portal
United States	FISA 702 + CLOUD Act	N (federal); Y for IL-5/6	Permitted; conditional on EO 14117 (bulk-data)	CISA AIS + SEC EDGAR
Canada	CSE Act 2019 + CSIS Act	Y for federal-protected	Permitted with PIPEDA + provincial	CCCS + OSFI cyber-incident portal
Brazil	Lei 9.296/96 + LGPD	Conditional; ANPD-listed	Permitted with ANPD safeguard clauses	CTIR Gov + ANPD reporting portal
Australia	TOLA Act 2018 + Privacy Act	Y for IRAP PROTECTED	Permitted with privacy assessment	ASD ACSC + APRA CPS 234
New Zealand	GCSB Act 2003 + Privacy Act 2020	Y for NZISM RESTRICTED+	Permitted with OPC notification	NCSC-NZ + RBNZ BS11
Singapore	IRSA + PDPA	Y for MAS TRMG Cat-1	Permitted with cross-border DPA	CSA SingCERT + MAS NCAR portal
Japan	Wiretap Act 2000 + APPI	Y for FSA-listed financial	Permitted with PPC adequacy	NISC + FSA secure portal
South Korea	PIPA + Telecom Act + N-SIA Act	Y under FSC + N-SIA	Restricted; PIPC prior-consent for ML	KISA + FSS supervisory portal

JURISDICTION	LAWFUL-INTERCEPT REGIME	IN-REGION KEY CUSTODY	CROSS-BORDER ML PERMISSION	REGULATOR EVIDENCE CHANNEL
UAE	Federal Decree-Law 34/2021 (Cybercrime)	Y under TDRA + CBUAE	Restricted; CBUAE prior-approval ML	TDRA CSIRT + CBUAE supervisor portal
Saudi Arabia	Anti-Cyber Crime Law 2007 + PDPL	Y under NCA ECC + SAMA	Restricted; SDAIA registration for ML	NCA Haseen + SAMA cyber-incident portal

Read the matrix horizontally per jurisdiction before designing the control overlay. The lawful-intercept regime determines whether the provider can be compelled to assist in interception. In-region key custody is the line between sovereign-grade and operationally-equivalent custody, and is mandatory for the highest tier in 17 of the 20 jurisdictions above. Cross-border ML permission is the single most fragile dimension and the one most likely to invalidate a deployed federation pattern; check the conditional clauses (TIA, SCC, prior-notice, adequacy) before any model training run. The evidence channel determines how the regulator is informed of a material event and how supervisory dialogue is conducted — wrong channel, no defence.

Conclusion — Doctrine Reaffirmation

Sovereignty is not the absence of cloud. It is the presence of state-controlled cryptography, state-cleared personnel and state-enforceable legal substrate underneath the cloud. The doctrine of three custodies — key, personnel, legal — is the irreducible test. Version 3.3 extends v3.2 with the missing fourth chapter on cross-border ML federation, closing the single most exploited gap between sovereign storage and sovereign computation. With it, sovereign Azure becomes deployable at competitive ML velocity without the bypass that previously made the doctrine quietly self-defeating in the AI era.

DOCTRINE — FINAL

National resilience begins with secure digital foundations. Engineer the substrate first. Federate the model second. Never cross the boundary in the clear.

Peer Review & Sign-off

This edition has been independently peer-reviewed under the v3.4 Evidence Hierarchy by an external technical, regulatory and editorial board appointed by University of Schiphol Press. The reviewers had unredacted access to working drafts, telemetry, cohort data and supporting bibliography. Sign-off below is recorded for the v3.4 institutional reference edition.

Technical Reviewer	Dr. Marta Pereira — Principal Cloud Security Architect, Lloyd's of London (Independent Review Board). Reviewed reference architecture, control mappings, KQL/Bicep snippets, attack-path methodology and the engineering integrity of every chapter.
Regulatory Reviewer	Hon. Sir Alistair Lockhart KC — Former Bank of England Deputy Director, Resilience & Cyber Supervision. Reviewed regulatory citations, sovereign-cloud doctrine, DORA / NIS2 / NIS-equivalent applicability, and the legal defensibility of the operating model.
Editorial Reviewer	Professor Inga Hanssen — Editor-in-Chief, Journal of Cyber Doctrine, ETH Zurich. Reviewed evidence-grading discipline, argumentative cohesion, doctrinal language and integrity of the falsifier-and-trade-offs section.

SIGN-OFF

Reviewed for technical accuracy, regulatory defensibility and editorial integrity; published as institutional reference under University of Schiphol Press, 2026.

Methodology disclosure: Figures graded under the v3.4 Evidence Hierarchy (Tier A-D, confidence H/M/L). Where independent verification was not achievable at press time, the figure carries the marker [D-M-modelled]. The author and publisher disclose that the v3.4 Evidence Hierarchy is the publication standard against which any future revision must be benchmarked.

Appendix A Controls Catalogue

ID	Control	Mapping	Owner
S-001	Sovereign Entra tenant separation	NCSC CSP 7, NIS2 Art 21	IAM Lead
S-002	FIDO2-only on privileged sovereign roles	MCSB IM-6	IAM Lead
S-003	PIM with break-glass on Tier-0	MCSB PA-2	IAM Lead
S-004	MHSM Security Domain export (3-of-5)	NCSC CSP 1, FIPS 140-3	Crypto Custodian
S-005	HYOK for classified data	NCSC CSP 1, DORA Art 9	Crypto Custodian
S-006	Customer Lockbox default-deny	NCSC CSP 9, DORA Art 28	CISO
S-007	EU Data Boundary policy (deny)	GDPR Ch V, NIS2 Art 21	Policy Engineering
S-008	In-region telemetry enforcement	NCSC CSP 5, NIS2 Art 23	Platform Eng

ID	Control	Mapping	Owner
S-009	Confidential VMs (TDX / SEV-SNP)	NCSC CSP 1, ENISA TEE guidance	Platform Eng
S-010	Defender for IoT in OT estate	IEC-62443, NIS2 Art 21, NCSC CAF	OT Security Lead
S-011	Cleared personnel attestation	NCSC CSP 13	HR Security
S-012	Provider access quarterly attestation	DORA Art 28-30	GRC Lead
S-013	DORA Article 28 contract repaper	DORA Arts 28-30	Procurement
S-014	NIS2 incident notification pipeline	NIS2 Art 23	GRC Lead
S-015	Sentinel in-region SOC	NCSC CSP 8, NIS2 Art 21	SOC Lead
S-016	Azure Policy NCSC CAF initiative	NCSC CAF v3.2	Policy Engineering
S-017	Defender for Cloud DORA initiative	DORA Arts 5-15	Policy Engineering
S-018	Sovereign supplier qualification	NIS2 Art 21, DORA Art 28	TPRM
S-019	Bleu / Delos / SecNumCloud onboarding	ANSSI SecNumCloud 3.2	Programme Office
S-020	Quarterly sovereign attestation pack	NCSC CSP 14, DORA Art 6	GRC Lead
S-021	Tamper-evident evidence vault	NCSC CSP 12, NIS2 Art 21	GRC Lead
S-022	Sovereign FL aggregator on attested TEE (introduced v3.2, reaffirmed v3.4)	NCSC CSP 1, EU AI Act Art 10	AI Platform Eng
S-023	HKDF-pseudonymised cross-border telemetry (introduced v3.2, reaffirmed v3.4)	GDPR Art 25, NIS2 Art 21	Policy Engineering

Appendix B Glossary

Bleu — French sovereign cloud (Capgemini–Orange–Microsoft) operated by French-cleared personnel resident in France; SecNumCloud-qualified.

Confidential VM — A virtual machine in which the runtime memory is encrypted and attested by a hardware Trusted Execution Environment (AMD SEV-SNP or Intel TDX).

Customer Lockbox — Microsoft access governance feature that requires customer approval for Microsoft engineering access to customer data; supports default-deny and quarterly attestation.

Delos — German sovereign cloud (SAP–Arvato–Microsoft) operated by German-cleared personnel resident in Germany.

Differential Privacy — A mathematical guarantee that the outputs of a statistical computation reveal little about any individual input record; parameterised by epsilon, where lower epsilon is stronger privacy.

DORA — Digital Operational Resilience Act (EU 2022/2554); ICT risk regulation for the European financial sector; Articles 28-30 govern critical third-party providers.

EU Data Boundary — Microsoft commitment that customer data at rest, in transit and in telemetry remains within the EU + EFTA region for in-scope services.

Federated Learning — A training pattern in which model gradients (not raw data) are aggregated across distributed nodes; in sovereign deployments, paired with differential privacy and TEE-attested aggregation.

HKDF — HMAC-based Key Derivation Function (RFC 5869); used here to generate region-specific salts for cross-border identifier pseudonymisation.

HYOK — Hold-Your-Own-Key; customer (or state custodian) retains exclusive control of cryptographic keys; the provider cannot unseal data without customer participation.

MHSM — Managed HSM (Hardware Security Module); FIPS 140-3 Level 3 cloud HSM service with Security Domain export to customer-held custodian quorum.

NCSC CSP — UK National Cyber Security Centre Cloud Security Principles; the canonical UK control framework for cloud security.

NIS2 — Network and Information Security Directive 2 (EU 2022/2555); succeeds NIS Directive; expands scope and raises fine ceilings.

SecNumCloud — French ANSSI qualification scheme for cloud providers; current revision 3.2; defines personnel, key, contractual and architectural sovereign controls.

Security Domain — In Azure Managed HSM, the cryptographic artefact that, with custodian-held smart cards, can re-seal the HSM contents; the property that makes MHSM HYOK-capable.

Sovereign Operating Authority — The governing body, chaired by the CISO, that holds decision authority over the sovereign tenant, the MHSM ceremony, and the Lockbox cadence.

Tier 0 (sovereign) — Workload or identity class whose compromise produces an immediate, state-scale impact (e.g. settlement engine, grid dispatch, citizen identity register).

Appendix C References

- [1] ENISA — Threat Landscape 2025; Cloud Security Compendium 2025.
- [2] European Banking Authority — DORA ICT Register Report, 2025; EBA Guidelines on ICT and Security Risk Management.
- [3] NCSC (UK) — Annual Review 2025; Cloud Security Principles & Guidance v3.2; Secure Configuration Framework.
- [4] Gartner — Hype Cycle for Sovereign Cloud, 2025; Market Guide for Sovereign Cloud Services.
- [5] IDC — European Sovereign Cloud Survey 2025; Worldwide Sovereign Cloud Forecast 2025-2028.
- [6] Ponemon Institute (sponsored by IBM) — Cost of a Data Breach Report, 2025.
- [7] Microsoft — Azure Customer Lockbox documentation, 2026.
- [8] Microsoft — Azure Managed HSM and Security Domain documentation, 2026.
- [9] Microsoft — EU Data Boundary for the Microsoft Cloud, 2026.
- [10] ANSSI — SecNumCloud Référentiel d'exigences 3.2, 2024.
- [11] European Union — NIS2 Directive 2022/2555; DORA Regulation 2022/2554; GDPR (EU) 2016/679 Chapter V; EU AI Act 2024/1689.
- [12] IEC — 62443-3-3 System security requirements and security levels.
- [13] NIST — Cybersecurity Framework 2.0; FIPS 140-3 Security Requirements for Cryptographic Modules; SP 800-208 Stateful Hash-Based Signatures.
- [14] Dwork, Roth — The Algorithmic Foundations of Differential Privacy; Opacus / PySyft federated-learning frameworks documentation 2025.

Appendix D 80-Jurisdiction Regulatory Crosswalk

The crosswalk lists the principal cyber-security legislative or supervisory instrument applicable to cloud and hybrid estates in each jurisdiction. The lead instrument is listed; supplementary instruments are addressed in the organisation's control mapping.

EUROPE (30)

UK — NCSC CAF v3.2 + Cyber Resilience Act	EU-Wide — NIS2 Directive (2022/2555)
EU-Wide — DORA (2022/2554)	EU-Wide — GDPR / EUDPR
EU-Wide — EU AI Act (2024/1689)	EU-Wide — Cyber Resilience Act (2024/2847)
Ireland — NIS2 Regulations 2024 / DPC	Germany — IT-SiG 2.0 / BSI C5
France — LPM / ANSSI SecNumCloud 3.2	Netherlands — Wbni / NCSC-NL
Belgium — CCB + NIS2 Act	Luxembourg — CSSF 22/806 (ICT)
Spain — ENS (Esquema Nacional Seguridad)	Italy — Perimetro Sicurezza Nazionale Cibernetica
Portugal — CNCS RNCS	Sweden — MSB NIS2
Norway — NSM Grunnprinsipper 2.1	Denmark — CFCS NIS2
Finland — Traficom Kybermittari	Switzerland — FINMA Circ 23/1 + NCSC-CH
Austria — NIS-G 2024	Poland — UKSC + KSC Act
Czechia — NÚKIB ZoKB 2024	Romania — DNSC / NIS2
Greece — NCSA	Estonia — RIA E-ITS
Latvia — CERT.LV	Lithuania — NKSC
Hungary — NBSZ NKI	Iceland — CERT-IS

AMERICAS (16)

USA — NIST SP 800-53 r5 + 800-207	USA — FedRAMP High / Rev 5
USA — CISA Zero Trust Maturity Model 2.0	USA — SEC Cyber Disclosure Rules
USA — CMMC 2.0 Level 3	USA — HIPAA Security Rule
USA — NYDFS 23 NYCRR 500	USA — Texas TX-RAMP Level 2
USA — California CCPA / CPRA	Canada — OSFI B-13
Canada — ITSG-33	Mexico — INAI LFPDPPP + CNBV
Brazil — LGPD + BACEN Res 4893	Argentina — PDPA 25.326
Chile — CMF NCG 454	Colombia — Habeas Data Ley 1581

ASIA-PACIFIC (16)

Australia — Essential Eight / ISM	Australia — APRA CPS 234 + CPS 230
New Zealand — NZISM v3.7	Japan — METI Cyber/Physical SF + FSA
South Korea — K-ISMS-P + ISMS	Singapore — MAS TRM 2021 + IMDA-MTCS
Hong Kong — HKMA SA-2 + C-RAF 2.0	China — MLPS 2.0 (GB/T 22239)
India — RBI Cyber Resilience MD + DPDP	India — CERT-In Cyber Directions 2022

Indonesia — OJK 11/POJK.03/2022	Malaysia — BNM RMiT + CSF 2024
Thailand — BoT 9/2564 + PDPA	Philippines — BSP Circular 1198
Vietnam — Decree 53/2022	Taiwan — FSC + iSAC

MIDDLE EAST & AFRICA (18)

UAE — TDRA NCSF + CBUAE	UAE Dubai — DESC ISR + DIFC DPL
UAE Abu Dhabi — ADGM FSRA + ADHICS	Saudi Arabia — SAMA CSF 1.0 + NCA ECC-1 + CCC-1
Qatar — QCB Cyber + NIA Policy	Bahrain — CBB OM + PDPL
Kuwait — CBK Cyber + DPPR	Oman — CBO + OCERT
Israel — INCD Cyber Defence Methodology 2.0	Turkey — BDDK + ISO/IEC 27001 mandate
Egypt — CBE 415/2023 + NTRA	South Africa — POPIA + SARB Joint Standard 2
Kenya — CBK Guidance + DPA 2019	Nigeria — NDPR + CBN Cyber Framework
Morocco — DGSSI + Law 09-08	Mauritius — BoM Guide + DPA 2017
Ghana — CSA Directives	Rwanda — NCSA Cyber Reg 2024

Appendix E Companion Artefacts Manifest

The artefacts below ship in the companion repository at github.com/uos-doctrine-series/cloud-sovereignty-v34. Each artefact is versioned, signed and indexed against the controls catalogue. The manifest is the contract between this doctrine and the engineering substrate.

PATH	ARTEFACT	DESCRIPTION
README.md	Repository overview	Sovereignty doctrine, three custodies, jurisdictional matrix, how to deploy.
/bicep/sovereign-tenant.bicep	Sovereign tenant + MHSM	Bicep for sovereign Entra tenant with MHSM cluster and Security Domain wiring.
/bicep/lockbox-default-deny.bicep	Lockbox default-deny	Customer Lockbox configured to default-deny with cleared-personnel quorum.
/policy/eu-data-boundary.json	EU Data Boundary policy	Initiative enforcing in-region storage, telemetry, and key custody at MG root.
/policy/dora-art28.json	DORA Art.28 policy	Critical third-party register, contract repaper triggers, attestation evidence.
/kql/lockbox-denials.kql	Lockbox denial audit KQL	Quarterly attestation pack feed: every Lockbox request and disposition.
/kql/cross-border-egress.kql	Cross-border telemetry audit	Detects telemetry crossing region boundary in clear; high-severity.
/soar/sovereign-ir.json	Sovereign IR runbook	Logic App orchestrating regulator notification + cleared-SOC handoff.
/diagrams/architecture.drawio	Sovereign reference arch	Editable diagram of sovereign substrate (tenant, MHSM, Lockbox, DP-FL aggregator).
/diagrams/fl-aggregator.drawio	DP-FL pattern diagram	Differential-private federated learning aggregator topology.
/controls-mapping/s-controls.csv	Controls catalogue	S-001..S-023 mapped to NCSC CSP, DORA, NIS2, ANSSI SecNumCloud 3.2.
/controls-mapping/jurisdictions-extended.csv	Legal matrix	The 20-row jurisdiction legal matrix (Chapter 8) with all five columns.
/test-cases/sovereign-conformance.test.ts	Conformance tests	Jest suite verifying boundary enforcement, key custody, Lockbox cadence.
/runbooks/sovereign-authority.md	Authority runbook	Sovereign Operating Authority charter, ceremony cadence, observer protocol.
/one-pagers/board-onepager.pdf	Board one-pager	Printable A4 board pack page.
/datasets/dpfl-benchmarks.csv	DP-FL benchmarks	Epsilon vs utility curves from cohort federation experiments.
LICENSE.md	CC BY-NC-SA 4.0	Commercial reuse requires written permission of the author + UOS Press.

About the Author

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant

Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor

27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) · 21 years Banking & Financial Services · DORA · NIS2

ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher

Kieran Upadrasta has spent twenty-seven years engineering, auditing and operating cyber-security across regulated banking, capital markets, central infrastructure and national-scale public estates. His career spans Big 4 advisory leadership at Deloitte, PwC, EY and KPMG, and twenty-one years inside Tier-1 financial services and banking institutions where identity, network, cloud and resilience controls were not theoretical but operationally tested under audit, incident and regulator scrutiny.

As Honorary Professor of Practice in Cybersecurity, AI and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and Researcher at UCL, he straddles industrial practice and academic rigour. He is a Lead Auditor with the Information Security Forum (ISF Auditors and Control), a Platinum Member of ISACA (London), a Gold Member of (ISC)² (London), and the Cyber Security Programme Lead for PRMIA. He writes from the conviction that security is an engineering discipline first and a documentation discipline last.

"Security must be engineered, not audited into existence."