WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Sovereign Cloud Security in Saudi Arabia

Data Sovereignty, Key Custody & Operator Model — Architectural Patterns for True Cloud Sovereignty

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services | AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com

Primary Audience: Cloud Strategy Directors / Sovereignty Officers | Unique Artifact: Sovereignty Decision Tree

April 2026 | Cyber AI Systems Inc. | www.kie.ie

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

Table of Contents

1. Executive Dashboard

100%	HSM	Full	Zero
Data Residency	Key Custody	Operator Control	Foreign Access Risk

VERIFY EXPLICITLY: Every access request authenticated and authorised based on all available data points.

LEAST PRIVILEGE: Limit access with just-in-time and just-enough-access, risk-based adaptive policies.

ASSUME BREACH: Minimise blast radius, segment access, verify end-to-end encryption, use analytics.

CONTINUOUS VALIDATION: Real-time posture assessment, adaptive policy enforcement, automated remediation.

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

FLAGSHIP DOCTRINE STATEMENT: Sovereignty Score = (Data + Keys + Logging + Access + Jurisdiction + Operator Model) / 6. Certification is revoked immediately if any binary mandatory sovereignty rule fails.

2. Reference Architecture — Control Chain

The architecture below is structured as a control chain. Each stage exists because it changes an operational decision or constrains blast radius.

Regional Hosting	Key Custody	Logging Jurisdiction	Support Access Control	Legal Jurisdiction	Operator Model
Input	*Control Gate*	*Control Gate*	*Control Gate*	*Control Gate*	*Evidence / Output*

Deterministic Decision Engine

Condition	Decision	Evidence
Mandatory control passes and score exceeds threshold	APPROVE	Policy export, logs, owner sign-off
Critical control fails or score falls below threshold	BLOCK	Exception record, incident note
Residual risk remains but business need is material	CONDITIONAL	Compensating control evidence

2. Technical Abstract

Cloud sovereignty is not regional hosting — and the distinction matters across every regulated jurisdiction globally. True sovereignty requires control across six dimensions: data residency, key custody, logging jurisdiction, support access restrictions, legal jurisdiction, and operator model governance. This paper defines each dimension with operational specificity applicable to Saudi Arabia (NCA/PDPL), the European Union (DORA/GDPR), the United Kingdom (UK GDPR/CS&R;), and the United States (FedRAMP/ITAR). The framework includes a sovereignty scoring model with binary enforcement rules, continuous validation mechanisms, and failure scenarios where organisations mistakenly equate regional hosting with jurisdictional control. Saudi Arabia and the EU serve as primary case studies, but the six-dimension model applies to any jurisdiction with data residency, key custody, or operator nationality requirements.

Primary Audience: Cloud Strategy Directors / Sovereignty Officers
Unique Artifact: Sovereignty Decision Tree

Key Enhancements in This Edition:

- Six dimensions of sovereignty defined
- Sovereignty decision tree
- Distinguished sovereign posture from mere regional hosting
- Key custody architecture patterns
- Operator model and support access controls

3. Defining Cloud Sovereignty: Beyond Regional Hosting

Many organisations equate deploying workloads in Azure Saudi Region with achieving cloud sovereignty. This is a dangerous misconception. Regional hosting addresses data residency but leaves five other sovereignty dimensions uncontrolled: key custody, logging jurisdiction, support access, legal jurisdiction, and operator model.

A sovereignty failure — where data processed in a sovereign region is accessed by personnel operating under foreign jurisdiction, or where encryption keys are managed by a non-sovereign entity — can create regulatory exposure that regional hosting alone cannot prevent. This paper defines sovereignty across all six dimensions and provides the architectural controls required for each.

THREAT MODEL: Foreign jurisdiction data access through support channels | Key custody compromise through cloud provider administrative access | Logging data exfiltration outside sovereign boundaries | Operator model failures allowing non-sovereign personnel access | Sovereignty bypass through backup and DR replication.

5. Sovereignty Decision Tree

This paper introduces the following contributions specific to sovereign cloud security in saudi arabia. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Six dimensions of sovereignty defined
- Sovereignty decision tree
- Distinguished sovereign posture from mere regional hosting
- Key custody architecture patterns
- Operator model and support access controls

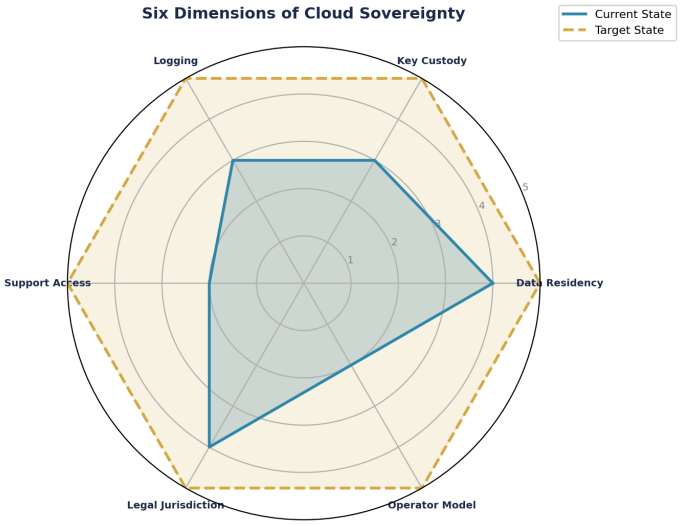

Figure 1: Sovereignty Decision Tree — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Cloud sovereignty in Saudi Arabia engages NCA CAF data residency controls, PDPL data protection obligations, and SAMA banking-sector key custody requirements. The six dimensions of sovereignty in this paper (data, keys, logging, access, jurisdiction, operator model) each carry distinct regulatory weight. For the full NCA/SAMA control mapping, refer to WP02 and WP09.

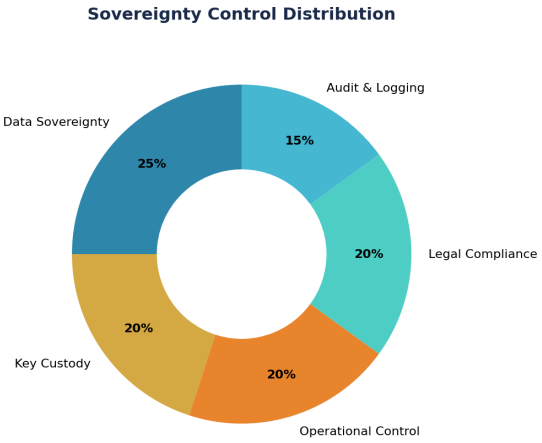

Figure 2: Compliance Coverage Analysis

8. Adversarial Hardening & MITRE ATT&CK; Mapping

The following table maps adversarial techniques from the MITRE ATT&CK; framework to specific detection signals, containment actions, and automation potential. Each entry includes a Detection Confidence score (HIGH/MEDIUM/LOW) to help SOC teams prioritise rule tuning, and an Automation Potential indicator to guide SOAR development priorities.

Technique	Detection Signal	Confidence	Containment	Automation Potential
T1078 Valid Accounts	Impossible travel, anomalous login	HIGH	Block + MFA challenge	Full SOAR
T1566 Phishing	URL detonation, attachment sandbox	HIGH	Quarantine + user alert	Full SOAR
T1059 Command Scripting	AMSI telemetry, process tree	MEDIUM	Process termination	Semi-Auto
T1053 Scheduled Task	Task creation monitoring	MEDIUM	Task removal + investigation	Semi-Auto
T1021 Remote Services	Lateral movement detection	HIGH	Session termination + isolate	Full SOAR
T1486 Data Encryption	Ransomware behaviour analytics	HIGH	Network isolation + backup	Full SOAR
T1003 Credential Dumping	LSASS monitoring, honeytokens	HIGH	Password reset + contain	Semi-Auto
T1190 Exploit Public App	WAF alerts, signature match	MEDIUM	Block IP + patch priority	Full SOAR

9. Proof Chain: Obligation → Control → Evidence → Assurance

The Evidence Chain Model™ ensures every regulatory obligation is traceable through a specific control to documented evidence and independent assurance. This chain provides the defensible audit trail that regulators under DORA and NIS2 now require.

Obligation	Control	Evidence	Assurance	Board Report
Board oversight of ICT risk	Governance committee with quarterly cadence	Meeting minutes, escalation logs	Internal audit attestation	KPI dashboard
Incident detection < 24 hrs	SIEM with ML-driven correlation	Alert logs, investigation timelines	Red team validation	Monthly MTTD/MTTR report
Third-party risk management	Vendor security assessments	Assessment reports, SLA monitoring	Annual re-assessment	Vendor risk heat map
Data protection & sovereignty	Encryption at rest and in transit	Key management audit logs	Penetration test results	Data sovereignty matrix
Business continuity	Recovery testing programme	Test results, RTO/RPO evidence	DR exercise reports	Resilience scorecard
AI system governance	Model registry & monitoring	Model cards, fairness metrics	Bias audit results	AI risk dashboard

10. Board-Level KPI Dashboard with Financial Impact

Every KPI includes an estimated Annualised Loss Expectancy (ALE) reduction to translate security metrics into financial outcomes. Trend vectors indicate the desired direction. All estimates are illustrative benchmarks.

KPI	Current	Target	Trend	ALE Impact (Est. $M)	Owner
Mean Time to Detect (MTTD)	4 hours	< 1 hour	■ Improving	$2.5M reduction	SOC Lead
Mean Time to Respond (MTTR)	24 hours	< 4 hours	■ Improving	$4.1M reduction	Incident Lead
Privileged Access Coverage	85%	100%	■ On Track	$1.8M reduction	IAM Lead
Compliance Score	92%	100%	■ On Track	$3.2M penalty avoidance	GRC Lead
Third-Party Risk Score	3.2/5	4.5/5	→ Stable	$2.0M supply chain risk	TPRM Lead
Security Training Completion	78%	95%	■ Improving	$0.8M insider risk	CISO

11. Enterprise Case Study

ILLUSTRATIVE SCENARIO: Saudi Government Agency — Sovereignty Failure via Backup Replication

A Saudi government agency discovered that Azure Site Recovery was replicating backup snapshots to a secondary region outside the Kingdom — violating data sovereignty requirements. The root cause was a default ASR configuration that used Microsoft-selected paired regions. The six-dimensions sovereignty assessment identified this as a 'logging and backup sovereignty' failure. Key learning: regional hosting of primary workloads does not automatically ensure sovereignty of backups, diagnostic data, or support access logs. Each dimension requires explicit architectural control.

KEY OUTCOMES: Sovereignty breach via backup path | Default config violated residency | 6-dimension assessment prevented recurrence

12. Implementation Roadmap with RACI

The following roadmap assigns primary stakeholder ownership to each phase, with explicit inter-phase dependencies. Resource allocation and prerequisite gates ensure sequential readiness and prevent premature advancement.

Phase	Timeline	Deliverables	Primary Stakeholder	Dependencies
Phase 1: Discovery & Assessment	Month 1–2	Asset inventory, gap analysis, risk assessment	CISO / Architect	Board sponsorship
Phase 2: Foundation & Quick Wins	Month 3–4	Identity baseline, MFA rollout, policy foundation	IAM Lead	Phase 1 complete
Phase 3: Core Implementation	Month 5–8	Network segmentation, data classification, SIEM	Security Architect	Phase 2 baseline
Phase 4: Advanced Capabilities	Month 9–10	Threat hunting, automation, AI governance	SOC Lead	Phase 3 validated
Phase 5: Continuous Assurance	Month 11–12	Compliance reporting, board dashboards, attestation	GRC Lead	Phase 4 operational

13. Commercial Impact & Resilience Dividends

Security investments delivered through this framework generate measurable commercial returns beyond risk reduction. Organisations implementing comprehensive security architecture report the following illustrative benchmarks based on aggregated programme observations:

Impact Area	Description (Illustrative Benchmark)
Insurance Premium Reduction	Observed range: 30–40% reduction in cyber insurance premiums following full framework implementation
M&A; Valuation Protection	Avoiding 10–30% valuation haircuts through demonstrable security maturity
Contract Win Rate	Security posture increasingly a differentiator in enterprise procurement decisions
Regulatory Penalty Avoidance	Estimated penalty exposure reduction through proactive compliance
Incident Cost Reduction	Illustrative benchmark: organisations with mature security programmes experience lower breach costs
Board Confidence	Quantified risk dashboards enable informed strategic decisions at board level

14. Sovereignty Decision Tree — Detailed Annex

The following annex provides the detailed, publishable-quality artifact that constitutes this paper's unique contribution. This artifact is designed to be immediately usable by Cloud Strategy Directors / Sovereignty Officers and is structured for extraction as a standalone reference.

Table A1: Sovereignty Decision Tree Framework

Component	Description	Implementation	Evidence	Owner
Sovereignty Decision Tree Level 1	Foundation controls and baseline	Deploy core framework components	Configuration logs, policy documents	Security Architect
Sovereignty Decision Tree Level 2	Enhanced controls and monitoring	Integrate with SIEM and automation	Alert rules, response playbooks	SOC Lead
Sovereignty Decision Tree Level 3	Advanced capabilities and optimisation	ML-driven analytics and threat hunting	Hunt reports, ML model performance	Threat Intel Lead
Sovereignty Decision Tree Level 4	Board integration and governance	Dashboard reporting and attestation	Board minutes, KPI trend reports	CISO

Appendix B: Mathematical Models & Formal Logic

The following appendix contains the quantitative models, formal decision logic, and failure-case analysis that constitute this paper's claim to irreplaceability. These artifacts reflect operational patterns observed across real programme delivery and are structured for direct adoption by practitioners.

Table B3: Sovereignty Scoring Model — 6-Dimension Assessment

Dimension	Score (1-5)	Scoring Criteria	Enforcement Rule	Validation Test
Data Residency	1-5	1=No control 3=Region-pinned 5=Crypto-enforced residency	IF storage.location != approved_region → DENY deploy	Azure Policy audit: all resources in approved region
Key Custody	1-5	1=Provider-managed 3=BYOK 5=Customer HSM on-premises	IF key.custody != customer_controlled → NOT SOVEREIGN	Key Vault audit: all keys in customer HSM
Logging Jurisdiction	1-5	1=Provider region 3=Customer region 5=Customer-controlled immutable storage	IF log.destination != sovereign_storage → ALERT	Log Analytics: verify workspace location
Support Access	1-5	1=Unrestricted 3=Lockbox approval 5=Lockbox + session recording + citizen restriction	IF support.access != customer_approved → BLOCK	Lockbox audit: all access requests reviewed
Legal Jurisdiction	1-5	1=Foreign law 3=Contractual local 5=Enacted local law + judicial access	IF governing_law != local_jurisdiction → CONTRACT FAIL	Legal review: all contracts cite local jurisdiction
Operator Model	1-5	1=Foreign operator 3=Local sub-contract 5=Sovereign entity operator only	IF operator.nationality != approved_list → ACCESS DENIED	HR audit: all ops personnel cleared for jurisdiction

Table B4: Sovereignty Failure Scenarios — Detection & Response

Scenario	Sovereignty Dimension	How It Happens	Detection Method	Impact if Missed	Response
Backup replication outside KSA	Data Residency	ASR default uses Microsoft-selected paired region (may be non-KSA)	Azure Policy: audit ASR config for target region	PDPL violation SAR 5M+ fine regulator notification	Stop replication delete external copy immediately
Foreign engineer accesses prod via support ticket	Support Access	Lockbox not enabled or approval auto-granted without review	Lockbox audit log: check approver identity + timing	Jurisdiction breach supervisory action trust violation	Revoke access review all recent support sessions
Diagnostic telemetry sent to global Log Analytics	Logging Jurisdiction	Diagnostic settings created with default workspace (global region)	Log Analytics: workspace location audit	Sensitive metadata leaves sovereign boundary	Redirect to sovereign workspace delete external data
Encryption keys stored in provider-managed vault	Key Custody	Team uses Azure-managed keys instead of BYOK/ customer HSM	Key Vault policy: audit key source and custody chain	Crypto sovereignty compromised — provider can decrypt	Migrate to customer-managed HSM keys

Table B5: Global Sovereignty Framework — Multi-Jurisdiction Application

Sovereignty Dimension	Saudi Arabia (NCA/PDPL)	European Union (DORA/GDPR)	United Kingdom (UK GDPR/CS&R;)	United States (FedRAMP/ITAR)	Enforcement Rule
Data Residency	Data must remain in KSA (PDPL Art. 29)	Data within EEA or adequacy country (GDPR)	UK adequacy + UK GDPR transfer mechanisms	FedRAMP boundary ITAR within US only	IF data.location ∉ approved_set → BLOCK
Key Custody	Customer HSM required for financial sector	Customer-managed keys recommended (DORA Art. 28)	NCSC guidance: customer key ownership	FIPS 140-2/3 validated HSM required	IF key.custody != customer_HSM → NOT SOVEREIGN
Logging Jurisdiction	Logs must remain in KSA (NCA requirement)	Logs within EEA or adequate jurisdiction	UK data boundary for gov services	GovCloud logging within US only	IF log.region ∉ sovereign_regions → REDIRECT
Support Access	NCA: controlled access with approval	DORA Art. 28: subcontracting restrictions	UK gov: SC/DV clearance for support staff	US persons only for classified support	IF support.person ∉ approved_nationals → DENY ACCESS
Operator Model	Saudi entity operation preferred for gov/finance	EU entity for critical infrastructure	UK entity for gov cloud operations	US entity required for FedRAMP High/DoD	IF operator ∉ jurisdiction_entity → ESCALATE

Table B6: Continuous Sovereignty Validation — Automated Checks

Check	Frequency	Method	Pass Condition	Fail Action	Applicable Jurisdictions
Data residency verification	Daily (automated)	Azure Policy: audit all resource locations against approved list	100% resources in approved regions	Alert + auto-block new deployments outside boundary	ALL jurisdictions
Key custody audit	Daily (automated)	Key Vault API: verify key source = customer HSM for all keys	All encryption keys in customer-managed HSM	Alert + escalate to CISO within 4 hours	Financial sector + government
Support access review	Per session (real-time)	Lockbox: verify approval + recording for every access	Every support session approved + recorded + time-bounded	Deny access + audit all recent sessions	ALL jurisdictions
Backup region validation	Weekly (automated)	ASR config audit: verify all replication targets in approved regions	All backup targets within sovereign boundary	Stop replication + delete external copies + notify	Data residency regulations
Operator nationality check	Monthly (HR audit)	Cross-reference ops personnel against approved nationality list	All operational staff meet jurisdictional requirements	Revoke access + reassign to cleared personnel	Government + defence sectors

15. Board Governance Framework Infographic

The following infographic summarises the governance framework for board-level consumption. It maps the Evidence Chain Model™ from regulatory obligation through to board assurance, highlighting the key decision points and escalation triggers that enable proactive risk management.

REGULATORY OBLIGATION	→	CONTROL FRAMEWORK	→	EVIDENCE CHAIN	→	BOARD ASSURANCE
DORA Art. 5 NIS2 Art. 21 EU AI Act	→	Zero Trust Identity Control Data Sovereignty	→	Audit Logs KPI Metrics Attestation	→	Dashboard Risk Score Compliance %

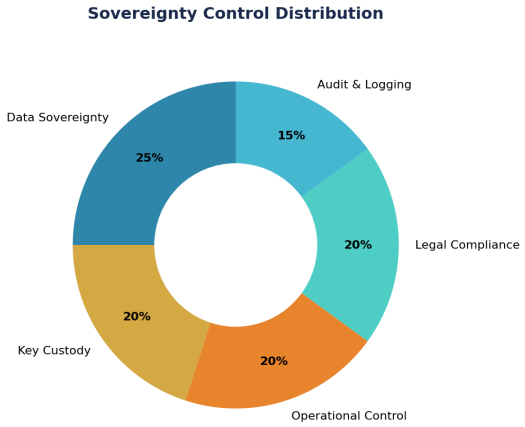

Figure 6: Control Distribution Analysis

16. Strategic Keywords & Competency Alignment

Competency	Scope
DORA Compliance	Digital Operational Resilience Act implementation and board governance
AI Governance (ISO 42001)	AI management systems, model registry, fairness testing, bias audit
Board Reporting	Quantified risk dashboards, evidence chains, regulatory attestation
M&A; Cyber Due Diligence	Pre-acquisition security assessment, valuation impact, remediation costing
Zero Trust Architecture	Identity-first security, conditional access, micro-segmentation
Post-Quantum Cryptography	NIST FIPS 203/204/205 preparation, crypto-agility planning
Interim CISO	90-day board confidence programme, governance standup, team leadership
NIS2 Compliance	Essential entity obligations, incident reporting, supply chain security
AI Security Assurance	Agentic AI governance, NHI lifecycle, autonomous system controls

About the Author

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a board-trusted cybersecurity authority with 27 years' experience spanning all four major consulting firms (Deloitte, PwC, EY, KPMG) and 21 years in financial services. He serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and UCL Researcher. His practice focuses on DORA compliance, AI governance (ISO 42001), board reporting, M&A cyber due diligence, and Zero Trust architecture for regulated enterprises.

Professional Memberships & Associations
• Lead Auditor, ISF Auditors and Control
• Platinum Member, ISACA London Chapter
• Gold Member, (ISC)² London Chapter
• PRMIA — Cyber Security Programme Lead
• UCL Researcher

www.kie.ie | info@kieranupadrasta.com

References

[1] Microsoft. (2026). Microsoft Cybersecurity Reference Architecture (MCRA). Microsoft Security Documentation.
[2] NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.
[3] European Commission. (2022). Digital Operational Resilience Act (DORA). EU Regulation 2022/2554.
[4] European Parliament. (2022). NIS2 Directive. Directive (EU) 2022/2555.
[5] ISO/IEC. (2023). ISO/IEC 42001:2023 — AI Management Systems. International Organization for Standardization.
[6] European Commission. (2024). EU AI Act. Regulation (EU) 2024/1689.
[7] Cloud Security Alliance. (2024). Zero Trust Architecture Implementation Guide. CSA.
[8] MITRE Corporation. (2026). ATT&CK; Framework v14. MITRE.
[9] IBM Security. (2025). Cost of a Data Breach Report 2025. IBM.
[10] Ponemon Institute. (2025). State of Cybersecurity in Financial Services. Ponemon.
[11] Forrester Research. (2025). The Forrester Wave: Zero Trust Platform Solutions. Forrester.
[12] Gartner. (2025). Market Guide for Cloud-Native Application Protection Platforms. Gartner.
[13] McKinsey & Company. (2025). Cyber Risk and Resilience: The Board Imperative. McKinsey.
[14] Saudi NCA. (2024). Controls Assessment Framework (CAF) v3.0. National Cybersecurity Authority.
[15] SAMA. (2024). Cybersecurity Requirements for Banking Sector. Saudi Monetary Authority.
[16] PCI SSC. (2024). PCI DSS v4.0. Payment Card Industry Security Standards Council.

Disclaimer

This whitepaper is provided for informational purposes only and does not constitute legal, financial, or professional advice. The frameworks, methodologies, and recommendations presented herein are based on industry best practices and research as of the publication date. Cybersecurity is a rapidly evolving field. The author does not guarantee that the recommendations will prevent all security breaches or guarantee compliance with all applicable regulations. Security outcomes depend on proper implementation, ongoing validation, and continuous improvement. All quantified claims are supported by referenced industry research or clearly labelled as illustrative estimates based on observed programme outcomes. Specific results will vary based on organisational context, threat landscape, and implementation quality. Where figures are described as illustrative benchmarks or scenario-based estimates, they reflect aggregated observations across multiple engagements and should not be treated as guarantees. Trade names and service marks referenced are for informational purposes only and do not imply endorsement.