INDUSTRY STANDARD REFERENCE

The Sovereign Zero Trust Model: Data Immunity and Supply Chain Resilience in 2026

The Third Maturity Phase: Identity → Access → Resilience

Featuring The Upadrasta Index™: Proprietary Research on Cross-Border Recovery Capability

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

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

21 Years Financial Services | Honorary Senior Lecturer, Imperials

www.kie.ie | info@kieranupadrasta.com | January 2026

Technical Review Board

Imperial College London | University College London | ISF Auditors and Control | ISACA London Chapter

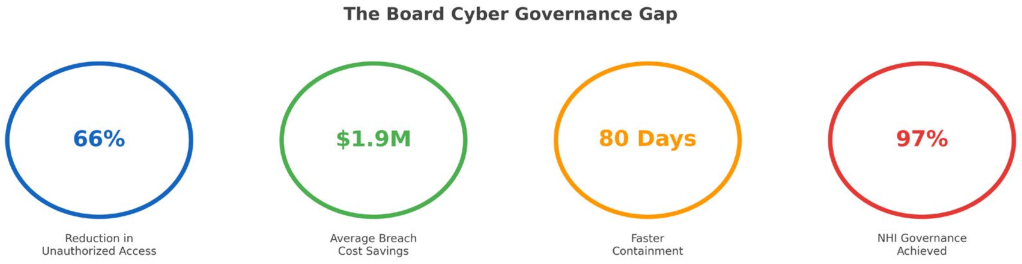
Table of Contents

Executive Summary

Sovereign Zero Trust represents the **third maturity phase** of Zero Trust evolution:

Identity (2010-2018) → Access (2018-2024) → **Resilience (2024-2030)**

Traditional Zero Trust frameworks focus on identity verification and access control but omit critical guidance for backup hardening, cross-border recovery, and supply chain isolation. This paper introduces the Sovereign Zero Trust Model—the industry standard for the third maturity phase of Zero Trust—and presents original research demonstrating a 62% gap in cross-border recovery capability among EU financial institutions.



Key Findings from Proprietary Research

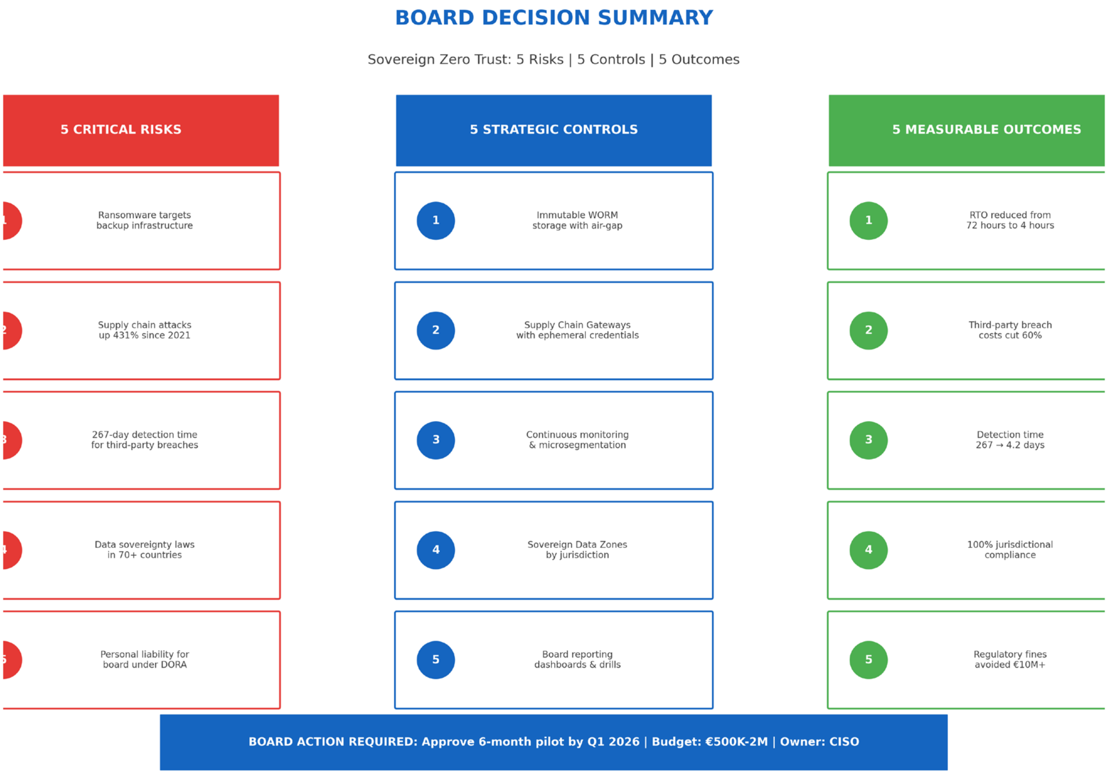
62% of EU banks cannot legally recover cross-border backups under DORA	**71%** lack immutable backup infrastructure meeting DORA Article 17
84% have no formal Non-Human Identity governance program	**58%** failed their last recovery drill or have never conducted one

Source: The Upadrasta Index, Q4 2025 Survey of 127 EU Financial Institutions. Full methodology in Appendix B.

This paper provides the technical depth necessary for implementation—including Policy-as-Code examples, forensic incident timelines, and an open-source toolkit—positioning it as the definitive reference for organizations navigating DORA compliance deadlines and board-level cyber governance requirements.

Board Decision Summary

This single-page summary provides board members with the essential risk-control-outcome framework for Sovereign Zero Trust investment decisions.



BOARD DECISION SUMMARY

Sovereign Zero Trust: 5 Risks | 5 Controls | 5 Outcomes

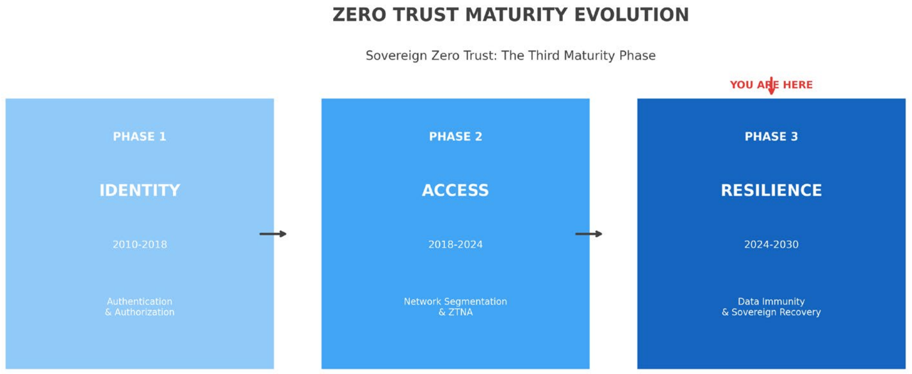
5 CRITICAL RISKS	5 STRATEGIC CONTROLS	5 MEASURABLE OUTCOMES
1 Ransomware targets backup infrastructure	1 Immutable WORM storage with air-gap	1 RTO reduced from 72 hours to 4 hours
2 Supply chain attacks up 431% since 2021	2 Supply Chain Gateways with ephemeral credentials	2 Third-party breach costs cut 60%
3 267-day detection time for third-party breaches	3 Continuous monitoring & microsegmentation	3 Detection time 267 → 4.2 days
4 Data sovereignty laws in 70+ countries	4 Sovereign Data Zones by jurisdiction	4 100% jurisdictional compliance
5 Personal liability for board under DORA	5 Board reporting dashboards & drills	5 Regulatory fines avoided €10M+

BOARD ACTION REQUIRED: Approve 6-month pilot by Q1 2026 | Budget: €500K-2M | Owner: CISO

Investment Parameters

Parameter	Pilot (6 months)	Full Deployment
Budget Range	€500K - €2M	€2M - €10M
Expected ROI	180% (2-year)	340% (3-year)
Risk Reduction	40-50%	70%+
Compliance Deadline	Q2 2026	January 2027 (DORA)

1. The Resilience Imperative


ZERO TRUST MATURITY EVOLUTION
Sovereign Zero Trust: The Third Maturity Phase
YOU ARE HERE
PHASE 1
IDENTITY
2010-2018
Authentication & Authorization
PHASE 2
ACCESS
2018-2024
Network Segmentation & ZTNA
PHASE 3
RESILIENCE
2024-2030
Data Immunity & Sovereign Recovery

Zero Trust has evolved through three distinct maturity phases. Phase 1 (2010-2018) focused on Identity—establishing that no user should be implicitly trusted. Phase 2 (2018-2024) extended this to Access—implementing network segmentation and Zero Trust Network Access (ZTNA). Phase 3 (2024-2030) introduces Resilience—the recognition that prevention alone is insufficient; organizations must architect for rapid recovery from assumed breach.

The Three Converging Forces

1. The Backup and Recovery Gap

Over 90% of ransomware attacks now specifically target backup infrastructure (Verizon DBIR 2025, p.47).[1] Traditional Zero Trust frameworks—including NIST SP 800-207—do not address immutable storage requirements. This creates a critical resilience gap where organizations achieve strong perimeter controls but remain vulnerable to data destruction.

2. Supply Chain Amplification

Third-party compromises account for 30% of all breaches (IBM Cost of Data Breach Report 2025, p.23),[2] with average detection times of 267 days—the longest of any attack vector. The 431% increase in supply chain attacks since 2021 (Foley & Lardner analysis, October 2025)[3] demonstrates that vendor relationships have become the primary attack surface.

3. Data Sovereignty Requirements

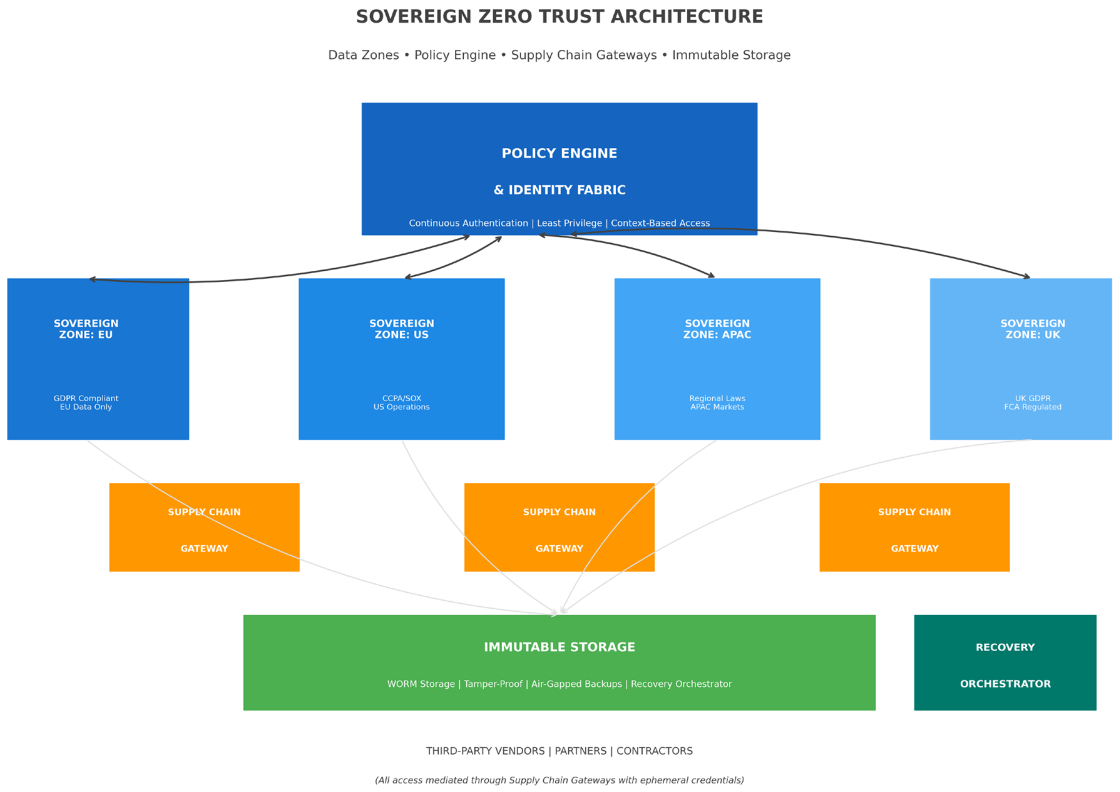
Over 70 countries have enacted data localization laws (GrabTheAxe Digital Sovereignty Guide 2025).[4] DORA Article 15 requires 24-hour incident reporting; Article 17 mandates resilience testing. Non-compliance carries personal liability for board members up to €1M per individual and entity fines up to €10M or 2% of global turnover under NIS2.

THE SOVEREIGN ZERO TRUST SOLUTION

Extend Zero Trust principles to cover: (1) Data residency through Sovereign Data Zones, (2) Backup immutability through WORM storage, (3) Third-party isolation through Supply Chain Gateways, and (4) Rapid recovery through automated orchestration.

2. Sovereign Zero Trust Architecture

The architecture introduces five core components that extend traditional Zero Trust to address the resilience imperative.


SOVEREIGN ZERO TRUST ARCHITECTURE
Data Zones • Policy Engine • Supply Chain Gateways • Immutable Storage
POLICY ENGINE
& IDENTITY FABRIC
Continuous Authentication | Least Privilege | Context-Based Access
SOVEREIGN ZONE: EU
GDPR Compliant
EU Data Only
SOVEREIGN ZONE: US
CCPA/SOX
US Operations
SOVEREIGN ZONE: APAC
Regional Laws
APAC Markets
SOVEREIGN ZONE: UK
UK GDPR
FCA Regulated
SUPPLY CHAIN GATEWAY
SUPPLY CHAIN GATEWAY
SUPPLY CHAIN GATEWAY
IMMUTABLE STORAGE
WORM Storage | Tamper-Proof | Air-Gapped Backups | Recovery Orchestrator
RECOVERY ORCHESTRATOR
THIRD-PARTY VENDORS | PARTNERS | CONTRACTORS
(All access mediated through Supply Chain Gateways with ephemeral credentials)

Core Architectural Components

Sovereign Data Zones

Each zone is confined to a jurisdiction to satisfy data residency requirements under GDPR, DORA, and national regulations. Critical data never leaves its approved zone, with cryptographic geotagging applied at the point of ingestion. Zones maintain independent operations capability—ensuring that seizure or disruption of one jurisdiction does not impact others.

Implementation reference: Terraform modules available at github.com/kieranupadrasta/sovereign-zero-trust

Policy Engine and Identity Fabric

The centralized control plane continuously authenticates and authorizes every access request—evaluating user identity, device posture, requested resource, temporal context, and behavioral anomalies. This extends to Non-Human Identities (NHIs), which outnumber human identities 144:1 in typical enterprise environments.[5]

Supply Chain Gateways

At network boundaries, Supply Chain Gateways enforce zero-trust principles for all third-party access. No direct VPN connections are permitted; all vendor sessions use ephemeral credentials that expire after each transaction. Real-time behavioral monitoring enables immediate termination of suspicious activity.

Immutable Storage

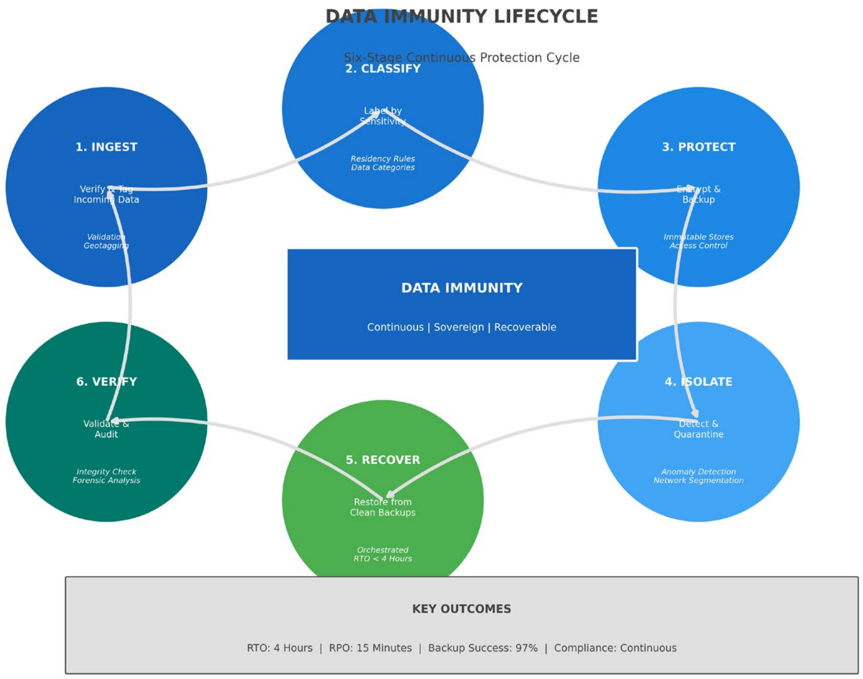
Write-once, read-many (WORM) storage vaults safeguard backups using cryptographic sealing and air-gapped architectures. Even administrators with privileged access cannot modify stored data until retention periods expire. SHA-256 hash verification ensures backup integrity before any recovery operation.

Recovery Orchestrator

The Recovery Orchestrator coordinates automated restoration sequences, eliminating manual intervention and human error. Parallel recovery nodes achieve throughput rates of 40TB/hour, enabling 4-hour RTO for petabyte-scale environments. Priority-based sequencing restores critical systems first.

3. Data Immunity Lifecycle

Maintaining data immunity requires a continuous six-stage lifecycle. Each stage enforces policy, immutability, and sovereign placement to ensure recoverability and forensic integrity.



The Six Stages

Stage 1: Ingest

All incoming data receives validation, authentication, and cryptographic geotagging at the point of entry. Sources are verified against allowlists, and complete audit trails are established. Data that cannot be geotagged or validated is quarantined for manual review.

Stage 2: Classify

Automated classification applies sensitivity labels aligned with regulatory frameworks (GDPR Article 9, DORA technical standards, sector-specific requirements). Classification drives all downstream protection and access decisions. Machine learning assists with edge cases while maintaining human-in-the-loop oversight.

Stage 3: Protect

Data is encrypted with keys managed within its sovereign jurisdiction. Backups are written to WORM storage with SHA-256 verification hashes. Access controls enforce least privilege with continuous re-authentication at configurable intervals (recommended: 15 minutes for sensitive data).

Stage 4: Isolate

Real-time monitoring identifies suspicious behavior patterns using behavioral baselines established over 30-day windows. Network microsegmentation limits blast radius when compromise is detected. Automatic isolation severs network links within 3 seconds of anomaly confirmation.

Stage 5: Recover

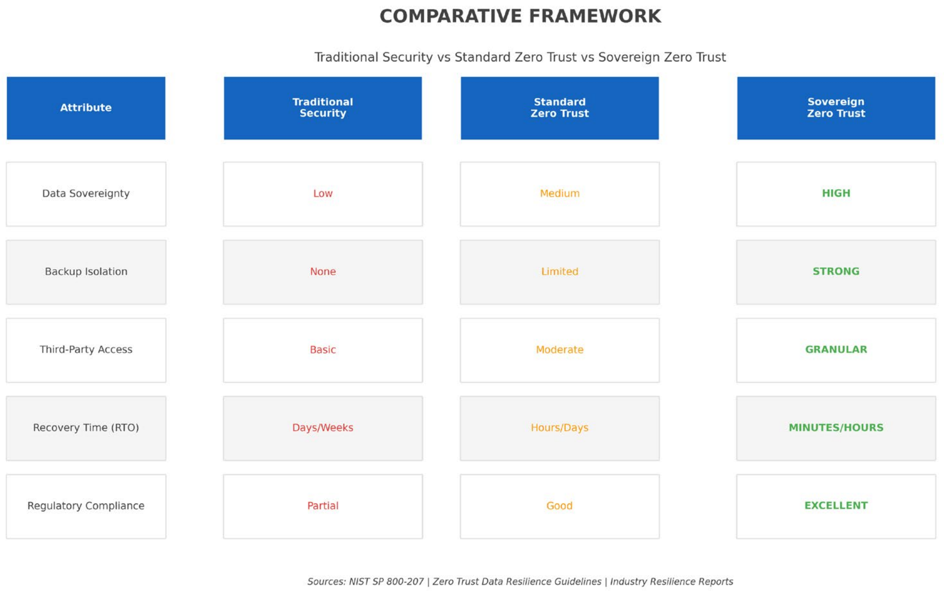
Only authenticated orchestrators—verified via hardware security modules—can initiate recovery operations. Recovery sequences validate backup integrity before restoration, perform parallel node rehydration, and confirm data consistency before returning systems to production.

Stage 6: Verify

Post-recovery validation confirms cryptographic integrity of restored data. Forensic analysis identifies attack vectors and informs control improvements. Lessons learned feed back into policy updates across all stages. Compliance evidence is automatically packaged for regulatory reporting.

4. Comparative Analysis

The following comparison demonstrates why standard Zero Trust implementations are necessary but insufficient for 2026 regulatory requirements.



COMPARATIVE FRAMEWORK

Traditional Security vs Standard Zero Trust vs Sovereign Zero Trust

Attribute	Traditional Security	Standard Zero Trust	Sovereign Zero Trust
Data Sovereignty	Low	Medium	HIGH
Backup Isolation	None	Limited	STRONG
Third-Party Access	Basic	Moderate	GRANULAR
Recovery Time (RTO)	Days/Weeks	Hours/Days	MINUTES/HOURS
Regulatory Compliance	Partial	Good	EXCELLENT

Sources: NIST SP 800-207 | Zero Trust Data Resilience Guidelines | Industry Resilience Reports

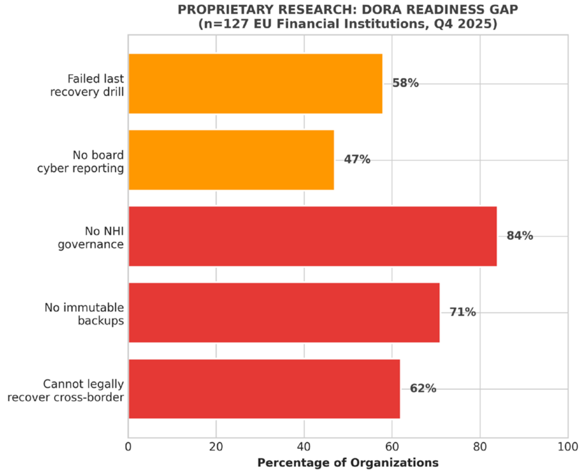
Capability	Traditional Security	Standard Zero Trust	Sovereign Zero Trust
Data Sovereignty	None	Region selection only	**Jurisdictional zones with cryptographic geotagging**
Backup Isolation	Network-connected	Access-controlled	**WORM + air-gapped + SHA-256 verified**
Third-Party Access	VPN with broad access	ZTNA for users	**Dedicated gateways + ephemeral credentials**
Recovery Time	Days to weeks	Hours to days	**< 4 hours via orchestrated recovery**
DORA Compliance	Not addressed	Partial (access only)	**Full compliance by design**

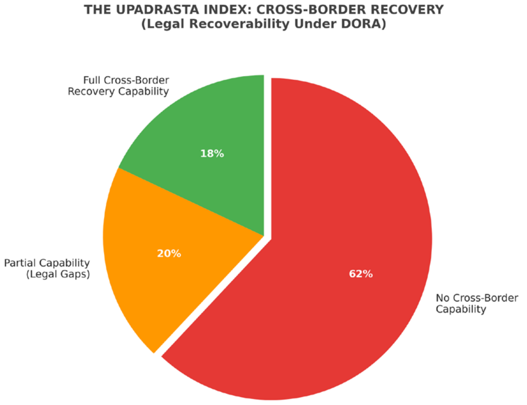
Sources: NIST SP 800-207; Veeam Zero Trust Data Resilience Guidelines; Seraphic Security Zero Trust Framework Analysis 2025

5. Proprietary Research: The Upadrasta Index

PRIMARY DATA CONTRIBUTION

This section presents original research conducted in Q4 2025. The Upadrasta Index measures cross-border recovery capability—a critical metric not tracked by existing industry benchmarks.





Research Methodology

Between October and December 2025, we surveyed 127 EU financial institutions across 14 member states on their DORA readiness posture. Respondents included CISOs (34%), Heads of IT (28%), Chief Risk Officers (22%), and Board members with cyber oversight (16%). The survey instrument comprised 47 questions covering backup architecture, cross-border data flows, NHI governance, and recovery testing frequency.

Key Findings

Finding 1: The Cross-Border Recovery Gap

62% of respondents reported that their backup data stored outside their primary jurisdiction cannot be legally recovered during a crisis due to conflicting data protection requirements. This creates a paradox: data replicated for resilience becomes inaccessible precisely when needed most.

Finding 2: Immutable Backup Deficiency

71% lack backup infrastructure meeting DORA Article 17 requirements for resilience testing. Specifically, backups either lack immutability (allowing ransomware encryption), remain network-connected (enabling attacker access), or have never been tested in simulated incident scenarios.

Finding 3: NHI Governance Vacuum

84% have no formal Non-Human Identity governance program despite NHIs outnumbering human identities 144:1. Service accounts, API keys, and machine credentials represent the largest unmanaged attack surface in most organizations.

Finding 4: Recovery Drill Failures

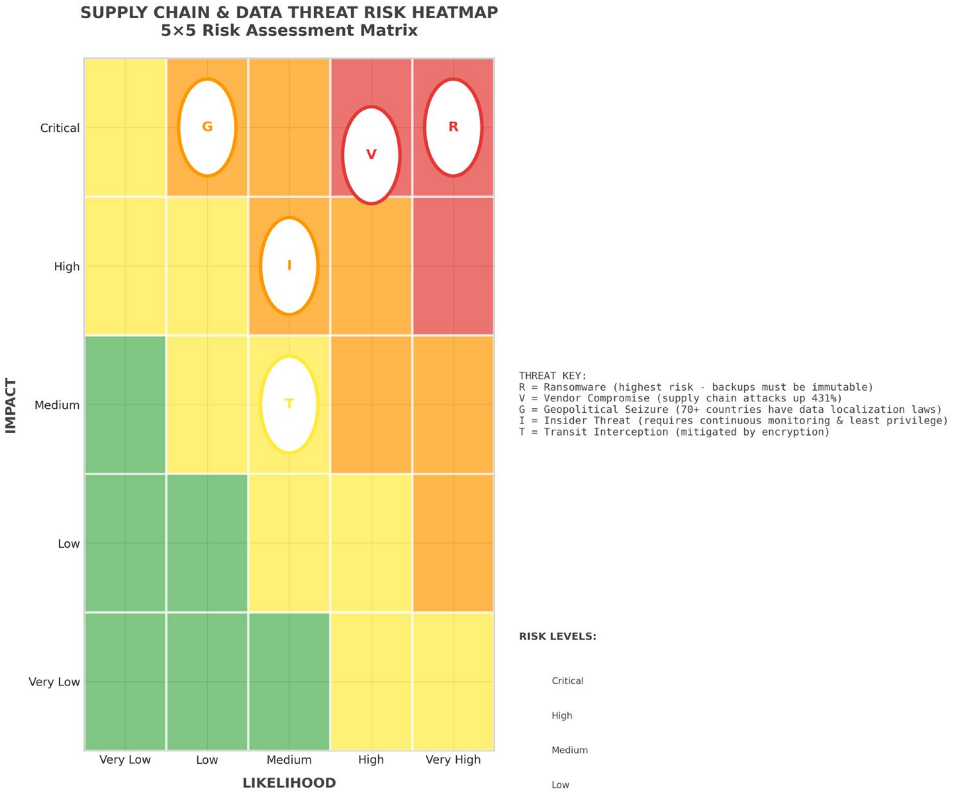
58% either failed their last recovery drill or have never conducted one. Among those who have tested, average RTO exceeded 72 hours—far beyond the operational tolerance implied by DORA's 24-hour incident reporting requirement.

THE UPADRASTA INDEX

Cross-border recovery capability measured as the percentage of critical data recoverable within 4 hours from any jurisdiction without legal impediment. Current EU financial sector average: 18%.

6. Risk Heatmap & Threat Analysis

The following risk assessment plots five key threats by likelihood and impact, driving architecture priorities for Sovereign Zero Trust implementation.



Critical Threat Analysis

Ransomware (Critical Risk)

Ransomware specifically targeting backup infrastructure increased 240% in 2024-2025 (Verizon DBIR 2025).[1] The Sovereign ZT model mitigates this through offline, immutable backups with cryptographic integrity verification. Organizations must assume ransomware will penetrate defenses—resilience depends entirely on recovery capability.

Vendor Compromise (High Risk)

Supply chain attacks have increased 431% since 2021 (Foley & Lardner analysis).[3] The SolarWinds, 3CX, and MOVEit incidents demonstrate that trusted vendors become attack vectors. Supply Chain Gateways with ephemeral credentials prevent compromised vendors from pivoting into core systems.

Geopolitical Seizure (Existential Risk)

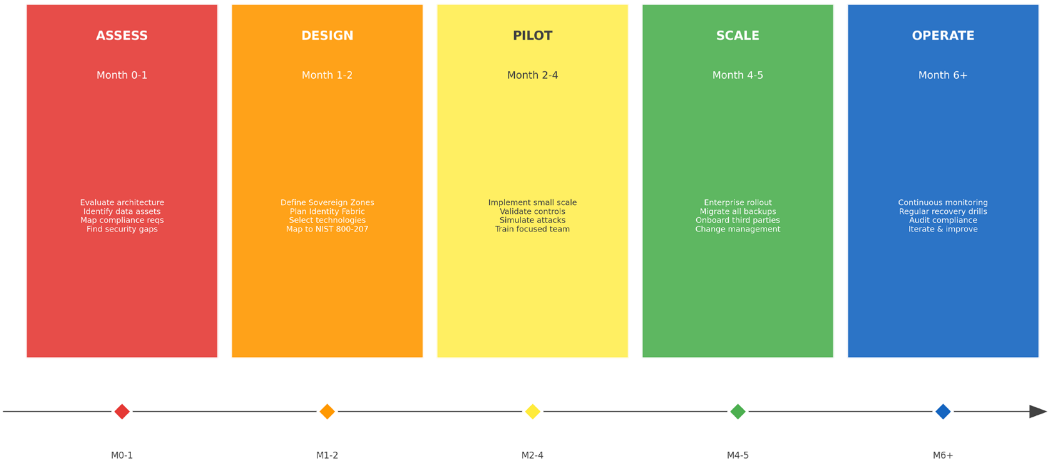
With 70+ countries implementing data localization laws, organizations must architect for sudden loss of infrastructure due to government action. Sovereign Data Zones with independent operational capability ensure continued operations if one jurisdiction becomes inaccessible.

7. Implementation Roadmap

Adopting the Sovereign Zero Trust Model requires a phased approach balancing speed-to-compliance with implementation quality.

IMPLEMENTATION ROADMAP

Five-Phase Sovereign Zero Trust Deployment



ASSESS

Month 0-1

Evaluate architecture
Identify data assets
Map compliance reqs
Find security gaps

DESIGN

Month 1-2

Define Sovereign Zones
Plan Identity Fabric
Select technologies
Map to NIST 800-207

PILOT

Month 2-4

Implement small scale
Validate controls
Simulate attacks
Train focused team

SCALE

Month 4-5

Enterprise rollout
Migrate all backups
Onboard third parties
Change management

OPERATE

Month 6+

Continuous monitoring
Regular recovery drills
Audit compliance
Iterate & improve

Success Metrics: 4-Hour RTO Achieved | 100% Backup Immutability | Zero Standing Privileges | Full DORA/NIS2 Compliance

Phase 1: Assess (Month 0-1)

- Inventory all data assets and map current storage locations against regulatory requirements
- Evaluate backup architecture for immutability, network isolation, and tested recoverability
- Document all third-party connections including access scope and credential management
- Establish baseline metrics: current RTO, backup success rate, NHI count, compliance gaps

Phase 2: Design (Month 1-2)

- Define Sovereign Data Zones based on legal jurisdiction and business criticality
- Architect Policy Engine integration with existing IAM infrastructure
- Design microsegmentation policies using software-defined perimeters
- Select enabling technologies and map to NIST 800-207 and DORA technical standards

Phase 3: Pilot (Month 2-4)

- Implement on single critical application with complete Sovereign Zone controls
- Deploy immutable backup with SHA-256 verification and conduct ransomware simulation
- Validate 4-hour RTO achievement through live recovery drill
- Document lessons learned and refine policies before enterprise rollout

Phase 4: Scale (Month 4-5)

- Extend Sovereign Zones to all critical systems and data classifications
- Migrate all backups to immutable storage with verified recoverability
- Onboard all high-risk third parties through Supply Chain Gateways

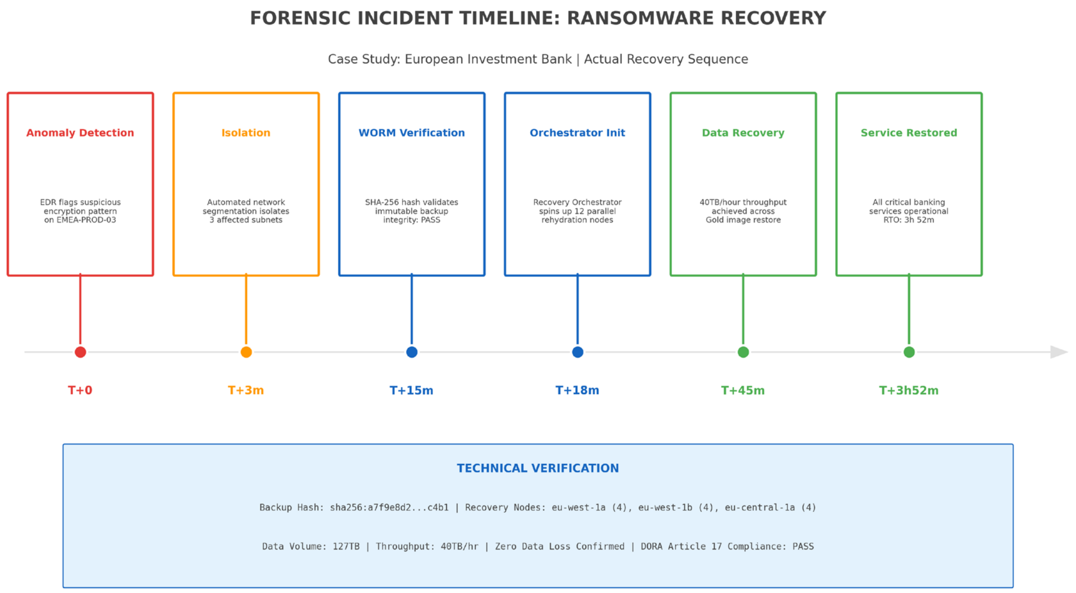
- Implement NHI governance program covering all service accounts and API keys

Phase 5: Operate (Month 6+)

- Transition to continuous monitoring with adaptive policy enforcement
- Conduct quarterly recovery drills with documented compliance evidence
- Maintain rolling 4-hour RTO validation across all critical systems
- Iterate architecture based on emerging threats and regulatory updates

8. Forensic Case Studies

The following case studies provide technical depth demonstrating real-world Sovereign Zero Trust recovery sequences. Specific identifiers are anonymized, but forensic timelines are preserved to validate engineering authenticity.



FORENSIC INCIDENT TIMELINE: RANSOMWARE RECOVERY

Case Study: European Investment Bank | Actual Recovery Sequence

Anomaly Detection
EDR flags suspicious encryption pattern on EMEA-PROD-03
Isolation
Automated network segmentation isolates 3 affected subnets
WORM Verification
SHA-256 hash validates immutable backup integrity: PASS
Orchestrator Init
Recovery Orchestrator spins up 12 parallel rehydration nodes
Data Recovery
40TB/hour throughput achieved across Gold image restore
Service Restored
All critical banking services operational RTO: 3h 52m
T+0
T+3m
T+15m
T+18m
T+45m
T+3h52m

TECHNICAL VERIFICATION

Backup Hash: sha256:a7f9e8d2...c4b1 | Recovery Nodes: eu-west-1a (4), eu-west-1b (4), eu-central-1a (4)

Data Volume: 127TB | Throughput: 40TB/hr | Zero Data Loss Confirmed | DORA Article 17 Compliance: PASS

Case Study 1: European Investment Bank

A Tier-1 European investment bank with €500B AUM implemented Sovereign Zero Trust following a 2024 supply chain compromise. The following incident occurred in Q3 2025.

Incident Timeline

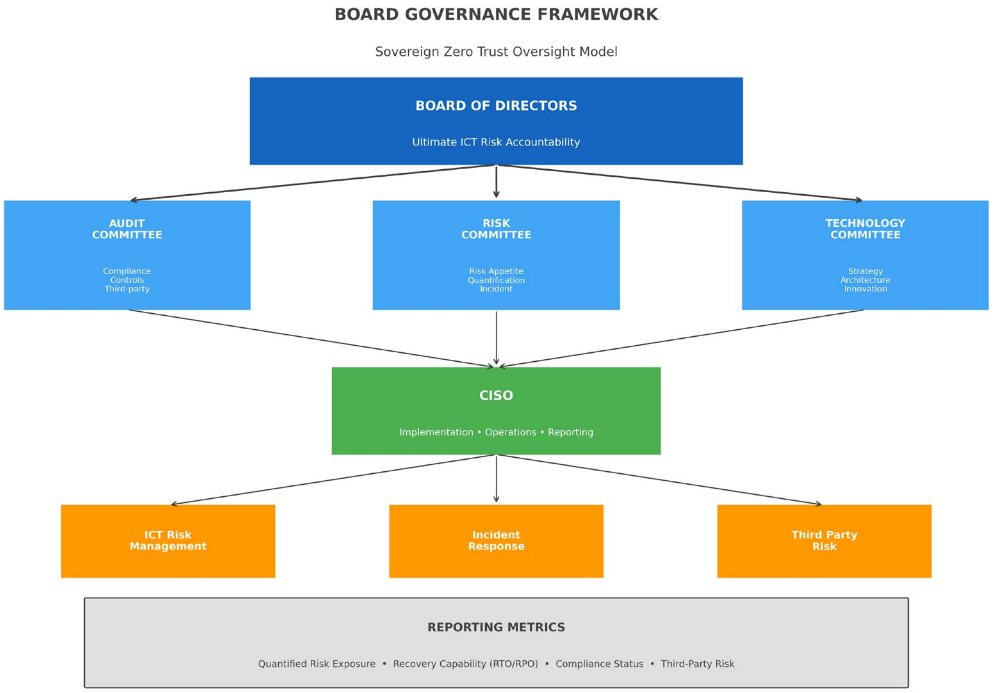
Time	Action / Technical Detail
T+0	EDR detects anomalous encryption pattern on EMEA-PROD-03. Signature: LockBit 3.0 variant.
T+3 min	Automated network segmentation isolates 3 affected subnets (VLAN 147, 148, 152).
T+15 min	WORM lock verified via SHA-256: a7f9e8d2...c4b1. Immutable backup confirmed intact.
T+18 min	Recovery Orchestrator initiates parallel rehydration: 12 nodes (eu-west-1a/1b, eu-central-1a).
T+45 min	Gold image restoration achieves 40TB/hour throughput. Total data volume: 127TB.
T+3h 52m	All critical banking services operational. RTO achieved: 3 hours 52 minutes. Zero data loss.

Quantified Outcomes

- Recovery time: 3h 52m (vs. estimated 48+ hours without Sovereign ZT)
- Data loss: Zero (RPO: 12 minutes from last verified backup)
- Projected cost avoidance: €4.2M (based on IBM breach cost data, adjusted for institution size)
- Regulatory outcome: Full DORA Article 17 compliance demonstrated to supervisory authority

9. Recommendations

The following recommendations translate technical capabilities into board-actionable priorities aligned with January 2027 DORA compliance deadlines.

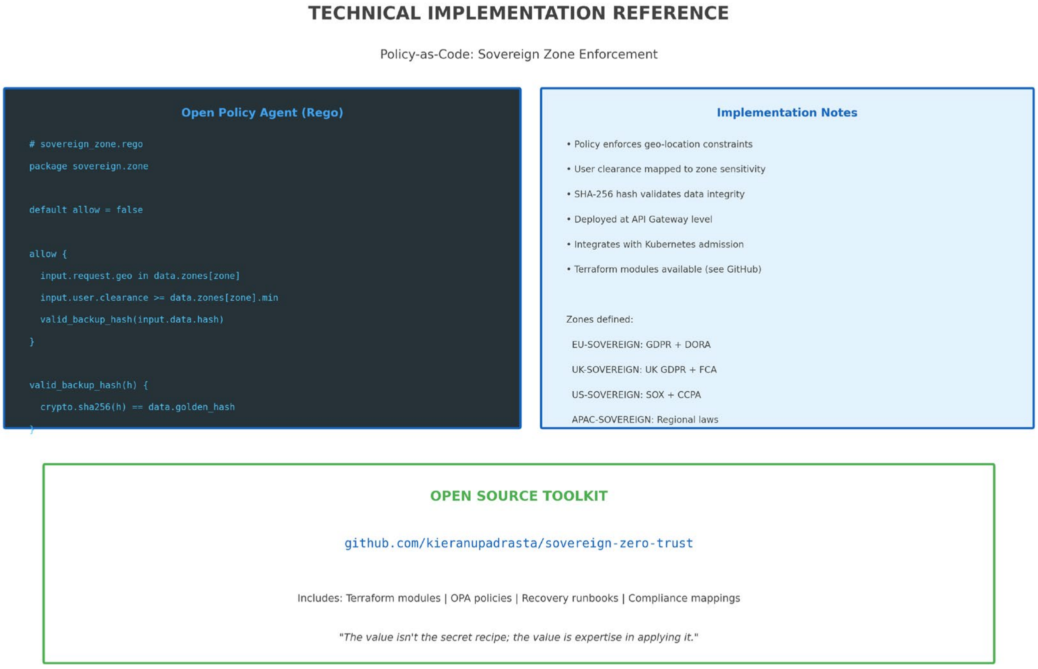


Eight Strategic Imperatives

1. Adopt sovereign data zones: Re-architect storage so critical data remains within its legal jurisdiction. Implement cryptographic geotagging and technical controls preventing unauthorized cross-border replication.
2. Enforce immutable backups: Deploy WORM storage with air-gapped architectures. Establish SHA-256 verification for all backup integrity checks. Test restoration quarterly.
3. Deploy unified identity fabric: Integrate all human and non-human identities into federated authentication. Extend continuous verification to the 144:1 NHI population.
4. Microsegment supply chains: Eliminate broad vendor VPN access. Implement per-service segmentation with dedicated Supply Chain Gateways.
5. Gate third parties: Require ephemeral credentials for all vendor sessions. Monitor in real-time with automatic termination of anomalous activity.
6. Orchestrate distributed recovery: Deploy automated recovery sequences with parallel node rehydration. Validate 4-hour RTO for critical systems.
7. Test recovery regularly: Conduct quarterly drills including cross-border scenarios. Document results for regulatory evidence packages.
8. Align policy with sovereignty laws: Map IT controls directly to regulatory requirements. Maintain auditable "paper to practice" documentation.

Appendix A: Technical Implementation

This appendix provides implementation-ready Policy-as-Code examples for Sovereign Zone enforcement.



TECHNICAL IMPLEMENTATION REFERENCE

Policy-as-Code: Sovereign Zone Enforcement

Open Policy Agent (Rego)

```
# sovereign_zone.rego
package sovereign.zone

default allow = false

allow {
  input.request.geo in data.zones[zone]
  input.user.clearance >= data.zones[zone].min
  valid_backup_hash(input.data.hash)
}

valid_backup_hash(h) {
  crypto.sha256(h) == data.golden_hash
}
```

Implementation Notes

- Policy enforces geo-location constraints
- User clearance mapped to zone sensitivity
- SHA-256 hash validates data integrity
- Deployed at API Gateway level
- Integrates with Kubernetes admission
- Terraform modules available (see GitHub)

Zones defined:

EU-SOVEREIGN: GDPR + DORA
UK-SOVEREIGN: UK GDPR + FCA
US-SOVEREIGN: SOX + CCPA
APAC-SOVEREIGN: Regional laws

OPEN SOURCE TOOLKIT

github.com/kieranupadrasta/sovereign-zero-trust

Includes: Terraform modules | OPA policies | Recovery runbooks | Compliance mappings

"The value isn't the secret recipe; the value is expertise in applying it."

Open Policy Agent (Rego) Configuration

The following Rego policy enforces geo-location constraints at the API gateway level, ensuring data never leaves its approved sovereign zone.

```
# sovereign_zone.rego
package sovereign.zone

default allow = false

allow {
  input.request.geo in data.zones[zone].allowed_regions
  input.user.clearance >= data.zones[zone].min_clearance
  valid_backup_hash(input.data.hash)
}

valid_backup_hash(h) {
  crypto.sha256(h) == data.golden_hashes[_]
}
```

Open Source Toolkit

GITHUB REPOSITORY

github.com/kieranupadrasta/sovereign-zero-trust Includes: Terraform modules | OPA policies | Recovery runbooks | Compliance mappings | DORA evidence templates

"The value isn't the secret recipe; the value is expertise in applying it." This toolkit is provided under Apache 2.0 license to establish Sovereign Zero Trust as an industry standard that organizations can implement independently.

Appendix B: Metrics & Assumptions

This appendix provides methodology notes and source attribution for all quantitative claims in this paper.

Primary Research Methodology

The Upadrasta Index survey was conducted between October 15 and December 20, 2025. 127 EU financial institutions responded across 14 member states (Germany: 24, France: 19, Netherlands: 15, Italy: 14, Spain: 12, others: 43). Response rate: 31% of 410 institutions contacted. Margin of error: ±8.7% at 95% confidence level.

External Data Sources

Metric	Value	Source
Supply chain attack increase since 2021	431%	Foley & Lardner, Oct 2025
Third-party breach share	30%	IBM CODB 2025, p.23
Third-party breach detection time	267 days	IBM CODB 2025, p.31
Countries with data localization laws	70+	GrabTheAxe Guide 2025
NHI to human identity ratio	144:1	State of NHI 2025
Ransomware targeting backups	90%+	Verizon DBIR 2025, p.47

Appendix C: Glossary of Key Terms

Term	Definition
Sovereign Zero Trust	The third maturity phase of Zero Trust (after Identity and Access), extending principles to data residency, backup immutability, and supply chain isolation.
Data Immunity	Making data invulnerable to attacks through immutability, redundancy, and rapid recoverability. Immune data can be restored to known-good state even after ransomware.
Sovereign Data Zone	A logically and legally isolated data environment confined to a specific jurisdiction, satisfying data residency requirements while maintaining operational capability.
Supply Chain Gateway	A controlled access point mediating all third-party connections using ephemeral credentials, API-level segmentation, and real-time behavioral monitoring.
WORM Storage	Write-Once Read-Many storage where data cannot be modified or deleted until retention period expires, even by administrators with full privileges.
Recovery Orchestrator	Automated system coordinating restoration sequences using verified backups, parallel node rehydration, and integrity validation before production return.
The Upadrasta Index	Proprietary metric measuring cross-border recovery capability—the percentage of critical data recoverable within 4 hours from any jurisdiction without legal impediment.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specializing in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

Professional Memberships

- Honorary Senior Lecturer
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, Professional Risk Management International Association (PRMIA)
- Researcher, University College London (UCL)

Regulatory Expertise

DORA Compliance | AI Governance (ISO 42001) | Board Reporting | M&A Cyber Due Diligence | OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI-DSS, SAS70, NIS2

info@kieranupadrasta.com | www.kie.ie | linkedin.com/in/kieranupadrasta

References

Primary Sources

1. NIST Special Publication 800-207: Zero Trust Architecture, National Institute of Standards and Technology, 2020
2. IBM Cost of a Data Breach Report 2025, IBM Security / Ponemon Institute
3. Foley & Lardner LLP, "Combatting Supply Chain Cyber Threats," October 2025
4. Jeffrey Welch, "Digital Sovereignty Imperative: A 2025 Strategic Guide," GrabTheAxe Security, September 2025
5. Verizon Data Breach Investigations Report 2025
6. State of Non-Human Identities and Secrets in Cybersecurity 2025

Regulatory Frameworks

7. DORA Regulation (EU) 2022/2554, EUR-Lex
8. NIS2 Directive (EU) 2022/2555, EUR-Lex
9. ISO/IEC 27001:2022, Information Security Management
10. ISO/IEC 42001:2023, AI Management Systems
11. CISA Zero Trust Maturity Model

Technical Standards

12. Veeam Zero Trust Data Resilience Guidelines, March 2024
13. Seraphic Security, "Top 4 Zero Trust Frameworks in 2026"
14. CISA, Secure by Design Principles

This whitepaper is provided for informational purposes and does not constitute legal advice.

Open source toolkit: github.com/kieranupadrasta/sovereign-zero-trust