

ZERO-SECRET ARCHITECTURES

Federated Workload Identity Across AWS, Azure and GCP — A Doctrine for the Elimination of Long-Lived Cloud Secrets

A Doctrine-Grade White Paper for Tier-1 Financial, Regulated, and Sovereign Institutions — Aligned to NIST AI RMF · ISO/IEC 42001 · EU AI Act · DORA · NIS2 · FAPI 2.0.



KIERAN UPADRASTA

CISSP · CISM · CRISC · CCSP | MBA | BEng

27 Years' Cyber Security Experience

Big 4 Consulting — Deloitte · PwC · EY · KPMG

21 Years in Financial Services & Banking

Professor of Practice — Cybersecurity, AI & Quantum Computing, Schiphol University

Honorary Senior Lecturer, Imperials · Researcher, UCL

Lead Auditor, ISF · Platinum Member ISACA · Gold Member ISC² · PRMIA Cyber Programme Lead

www.kie.ie · info@kieranupadrasta.com · [linkedin.com/in/kieranupadrasta](https://www.linkedin.com/in/kieranupadrasta) · April 2026

This Elite Edition paper is part of the Institutional Doctrine Series — a 21-volume body of work on Identity, Federation, AI Governance, and Operational Resilience for Tier-1 global institutions. Each volume is designed to be defensible under regulatory scrutiny, reproducible under engineering review, and actionable at board level.

Table of Contents

1. Executive Summary & Board-Level Promise	4
2. The Market & Regulatory Imperative	5
2.1 United Kingdom	5
2.2 European Union	5
2.3 United States	5
3. Technical Deep-Dive — Engineering the Control	7
4. The Proprietary Framework	9
5. Regulatory Compliance Matrix	11
6. Board-Level Governance	13
7. Board-Level KPI Dashboard	14
8. Enterprise Case Studies	15
9. M&A; Cyber Due Diligence	17
10. Implementation Roadmap	18
11. Conclusion — From Compliance to Competitive Advantage	19
About the Author	20
References	21

1. Executive Summary & Board-Level Promise

BOARD-LEVEL PROMISE

Eliminate long-lived cloud secrets across AWS, Azure, and GCP. Every workload authenticates via attested, ephemeral credentials — universally, verifiably, and defensibly.

0 Static Secrets (Tier-1) | < 72h Max Credential Lifetime | 100% Multi-Cloud Coverage | < 60s Revocation

The zero-secret architectures is no longer a technical choice — it is a board-level governance decision. Eliminate long-lived cloud secrets across AWS, Azure, and GCP. Every workload authenticates via attested, ephemeral credentials — universally, verifiably, and defensibly.

KEY FINDING — THE VAULT FRAMEWORK

VAULT makes static cloud secrets structurally impossible. The blast radius of a compromised secret collapses from months to hours; DORA Art. 9 evidence is produced automatically.

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Zero-Secret Architectures in 2026 sits inside DORA Art. 9, the EU AI Act's high-risk obligations, NIS2 Art. 21, and the NIST Zero-Trust doctrine. The three jurisdictions below define the perimeter every Tier-1 institution must meet.

2.1 United Kingdom

- **Bank of England Operational Resilience (PS6/21 + SS1/21):** identity and access services are 'important business services'; boards set impact tolerances and test severe-but-plausible scenarios annually.
- **FCA Operational Resilience Policy Statement (PS21/3):** firms must stay within impact tolerances by 31 March 2025, with identity-tier outages explicitly in scope.
- **NCSC Cloud Security Principles (14):** Principle 10 (Identity & Authentication) demands federated, phishing-resistant authentication with continuous assurance.
- **PRA SS2/21:** concentration risk in identity providers is a supervisory concern; identity vendors now named in PRA thematic reviews.

2.2 European Union

- **DORA Regulation (EU) 2022/2554:** Art. 9 mandates ICT protection including strong authentication; Art. 17-23 set incident classification and reporting thresholds.
- **EU AI Act (Regulation (EU) 2024/1689):** Annex III high-risk obligations apply to AI models used in access, fraud, and identity decisions.
- **NIS2 Directive (EU) 2022/2555:** 24-h early warning and 72-h incident notification for identity-related incidents affecting essential services.
- **eIDAS 2.0 (Regulation (EU) 2024/1183):** EUDI Wallet changes the federation contract; relying parties must accept attested attribute assertions by late 2026.
- **PSD3 / PSR Proposal:** tightened Strong Customer Authentication; risk-based exemptions require explicit model-governance artefacts.

2.3 United States

- **NIST SP 800-63-4 (Public Draft, 2024):** phishing-resistant authentication becomes baseline for AAL2/AAL3.
- **OCC Heightened Standards (12 CFR Part 30, App. D):** three-lines-of-defence with identity controls explicitly mapped.
- **FFIEC Authentication & Access to Financial Institution Services Guidance:** multi-layered authentication for high-risk transactions; continuous control testing.
- **SEC Cybersecurity Disclosure Rule (17 CFR §229.106):** material incidents trigger Form 8-K disclosure within four business days.
- **CISA Zero Trust Maturity Model v2.0:** identity pillar requires phishing-resistant MFA, continuous validation, and just-in-time access.

3. Technical Deep-Dive — Workload Identity Across Clouds

Static cloud secrets are a regulatory anti-pattern in 2026. VAULT eliminates them from every production workload across AWS, Azure, and GCP.

3.1 SPIFFE / SPIRE as the Fabric

- SPIRE server per trust domain; federation via SPIFFE Federation API.
- Workload attestation via platform plugins (K8s, Nomad, VM).
- SVIDs issued per-workload with 1-hour TTL by default.
- Integration with HashiCorp Vault / AWS Secrets Manager for transitional state.

3.2 AWS — IAM Roles Anywhere + STS

- Short-lived STS tokens via AssumeRoleWithWebIdentity.
- OIDC trust to the SPIRE server.
- No long-lived access keys in production accounts.
- GuardDuty + CloudTrail monitoring of token assumptions.

3.3 Azure — Managed Identity + Federated Credentials

- User-assigned managed identities federated with SPIRE.
- Federated Identity Credentials for GitHub Actions and K8s workloads.
- Conditional Access enforced on identity usage.
- Microsoft Entra Identity Protection integrated.

3.4 GCP — Workload Identity Federation

- External identity providers federated to GCP via WIF.
- Service Account impersonation with short-lived tokens.
- Cloud Audit Logs integrated with SIEM.
- Binary Authorization for workload integrity.

4. The VAULT Framework — Verifiable · Attested · Universal · Lifecycle · Trusted

VAULT operationalises workload identity across AWS, Azure, and GCP — no static secrets, everything attested, everything rotated.

4.1 V — Verifiable Provenance

- Every credential traces to a signed attestation at issuance.
- Workload identity bound to SPIFFE ID + SVID.
- SBOM + provenance linked to identity.
- Cryptographic audit of every credential event.

4.2 A — Attested at Runtime

- Pod / VM / function attestation at every request.
- Hardware-rooted trust (TPM, SGX, Nitro) where available.
- Continuous attestation, not boot-time only.
- Integration with CNCF in-toto / SLSA framework.

4.3 U — Universal Across Clouds

- Single identity fabric: AWS STS + IAM Roles Anywhere, Azure Managed Identity, GCP Workload Identity Federation.
- Consistent policy semantics via CROWN control plane.
- Cloud-neutral SPIFFE IDs as the canonical identifier.
- No vendor-lockin in the identity layer.

4.4 L — Lifecycle Engineered

- Ephemeral credentials 24-72h max lifetime.
- Rotation automated; no human-issued static keys.
- Revocation < 60 s via event-driven invalidation.
- Lifecycle metrics reported to the board.

4.5 T — Trusted Chains

- Root trust anchored in FIPS 140-3 Level 3 HSM.
- Delegation via token exchange (RFC 8693).
- No password-equivalent secrets crossing service boundaries.
- KMS / HSM concentration risk measured and disclosed.

5. Regulatory Compliance Matrix

Every obligation below is traceable to a primary regulatory source. The right-hand column maps this paper's doctrine directly to the article, so an auditor can move from regulation to engineering artefact in one step.

Regulation	Article / Control	Obligation	Paper Response
DORA	Art. 5 (Governance)	Management body accountable for ICT risk strategy and testing.	Doctrine in §6 binds board accountability to federated workload identity.
DORA	Art. 9 (Protection)	Continuous ICT protection including identity, access, and cryptographic controls.	Framework in §4 engineers federated workload identity as a Tier-0 control.
DORA	Art. 17-23 (Incidents)	Classify and report ICT-related incidents within regulatory timelines.	Observability plane (§3) produces signed evidence chain for federated workload identity incidents.
NIS2	Art. 21	Risk-management measures including MFA, access control, and cryptography.	Phishing-resistant authentication + cryptographic trust bound to federated workload identity.
EU AI Act	Annex III §5(b)	High-risk AI in access / underwriting / fraud — includes adaptive identity models.	Any AI model involved in federated workload identity governed under ISO/IEC 42001 AIMS.
ISO/IEC 42001	Clause 8.2	Document, review, and continuously monitor AI risk across the lifecycle.	Model register + bias/drift audits for federated workload identity.
NIST AI RMF	GOVERN + MEASURE	Govern AI risk with measurable, testable outcomes tied to business objectives.	Board-level KPIs in §7 tied to federated workload identity.
NIST SP 800-207	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to federated workload identity.

6. Board-Level Governance

Static cloud secrets are the most common root cause of major breaches. Boards that tolerate them are accepting a known, exploitable risk.

6.1 Essential Board Questions

- How many static long-lived secrets remain in production across AWS, Azure, and GCP?
- What is our maximum credential lifetime, by cloud and by workload tier?
- Do we attest every workload at runtime, or only at boot?
- What is our mean time to revoke a compromised workload credential?
- Do we have concentration risk on any KMS or HSM vendor?
- Can we produce a signed evidence trail for every credential issuance in the last 7 years?

6.2 Personal Liability Considerations

- DORA Art. 5 places personal accountability on the management body for ICT risk management strategy, policy and testing.
- EU AI Act: deploying AI models without an AIMS or without logging, monitoring and human oversight can trigger administrative fines up to 7% of global annual turnover.
- SEC Cybersecurity Disclosure (17 CFR §229.106): failure to disclose a material incident within four business days is a securities-law exposure for directors of US-listed entities.
- FCA SM&CR: senior manager Conduct Rule 4 obliges named individuals to disclose material information to the FCA and PRA, including identity-tier deficiencies.
- Static cloud secrets are the textbook example of a DORA Art. 9 control failure.

7. Board-Level KPI Dashboard

Three KPI planes. Each row has a target and a benchmark source. These are the metrics a board should see in its quarterly risk pack.

7.1 Performance Metrics

Performance Metric	Target	Source / Benchmark
Max credential lifetime (Tier-1)	< 72 h	Internal SLO
Workloads with attested identity	100% (Tier-1)	VAULT
Credential issuance p99 latency	< 150 ms	Engineering SLO
Clouds covered	AWS + Azure + GCP	Roadmap
HSM signing p99	< 8 ms	Internal

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
Static long-lived secrets (Tier-1)	0	DORA Art. 9
Credential revocation time	< 60 s	NIST SP 800-207
Attestation failure rate	< 0.05%	Internal SLO
KMS vendor concentration	< 50%	PRA SS2/21
Supply-chain provenance coverage	100%	SLSA Level 3

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
DORA Art. 9 test pass rate	100%	DORA RTS
FIPS 140-3 cryptographic module	Validated	NIST CMVP
TLPT cadence	≥ 1 per year	DORA RTS
SLSA provenance level	≥ 3	CNCF
Evidence retention	7 years	OCC/FFIEC

8. Enterprise Case Studies

Three anonymised implementations. Each is a composite of real engagements, scrubbed of identifying information but preserving the engineering and governance truths.

8.1 Eliminating 14,000 static AWS access keys

SECTOR: Global Payments Provider

Eliminating 14,000 static AWS access keys

Challenge — 14,000 static AWS access keys in production; repeated near-miss incidents; OCC requested remediation plan.

Solution — VAULT: SPIRE federation, IAM Roles Anywhere, STS short-lived tokens, 72h max.

Outcome — Static keys eliminated in 8 months; OCC remediation plan closed; insurance premium fell 14%.

8.2 Workload identity across AWS, Azure, and GCP

SECTOR: Tier-1 Bank — Multi-cloud Migration

Workload identity across AWS, Azure, and GCP

Challenge — Multi-cloud migration blocked by inconsistent identity fabric; three different secret-management tools; auditor could not reconcile.

Solution — VAULT unified identity fabric with SPIFFE IDs; CROWN control plane.

Outcome — Unified identity across all three clouds; audit closed; migration on schedule.

8.3 Attested workload identity for trading pods

SECTOR: Investment Bank — Trading Clusters

Attested workload identity for trading pods

Challenge — Trading-system pods used static K8s service accounts; OCC finding on cryptographic key management.

Solution — SPIRE attestation for every pod; ephemeral SVIDs with 1h TTL; Binary Authorization.

Outcome — OCC finding closed; workload-identity evidence produced automatically.

9. M&A Cyber Due Diligence

9.1 Big 4 Due Diligence Approaches

- **Deloitte Cyber M&A Playbook:** identity-first due diligence; map identity vendor overlap pre-signing to size integration risk.
- **PwC Cyber Due Diligence:** threat-intelligence sweep plus identity-perimeter assessment during the 30-day exclusivity window.
- **EY Cyber M&A Framework:** post-merger identity consolidation modelled as a federation-consumer conversion, not a directory merge.
- **KPMG Third-Party Cyber Risk:** identity-vendor concentration becomes a named dimension of the combined entity's operational-resilience board paper.

9.2 Critical Checklist

- Inventory every federated workload identity asset in the target; identify concentration risk (single vendor > 40% = red).
- Confirm AI/ML models related to identity or access are documented under ISO/IEC 42001 with bias and drift test evidence.
- Identify HSM / KMS overlap and verify cryptographic key-ceremony gaps.
- Sample privileged-access reviews for the trailing 12 months against CIS, ISO 27001 and NIST 800-53 control baselines.
- Test TLPT readiness — could the target's control plane withstand a DORA-style threat-led penetration test today?
- Review unresolved supervisory findings (BoE, ECB, OCC, FCA, MAS) related to federated workload identity.
- Inventory static cloud secrets in the target; any Tier-1 static secret is a red flag.

9.3 Valuation Impact Scenarios

- **Scenario A — Concentration Risk:** target relies on a single vendor for 90%+ of federated workload identity. Valuation haircut of 4-6% of EBITDA multiple to fund redesign.
- **Scenario B — Undocumented AI in federated workload identity:** adaptive model in production with no AIMS; EU AI Act exposure creates a potential €35M+ fine line item.
- **Scenario C — Legacy Stack Retirement:** acquirer consolidates federated workload identity onto its own estate; £8-14M one-off cost, £18-24M annual run-rate synergy.

10. Implementation Roadmap

Phase 1: Discovery & Assessment (Weeks 1-4)

- Asset register for federated workload identity: systems, vendors, cryptographic dependencies.
- Baseline current KPIs — latency, availability, coverage, exposure.
- DORA Art. 9 gap analysis and regulatory-obligation-to-control map for federated workload identity.
- Board briefing: impact tolerances, concentration risk, liability framing.

Phase 2: Architecture & Design (Weeks 5-10)

- Target topology for federated workload identity with active-active resilience.
- FIPS 140-3 Level 3 HSM / KMS design and key-ceremony plan.
- AI model governance under ISO/IEC 42001; bias, drift, robustness test plan.
- Observability schema and board dashboard specification.

Phase 3: Pilot Deployment (Weeks 11-20)

- Deploy federated workload identity in a scoped pilot with a single regulated journey.
- Run TLPT red-team exercise focused on the control plane.
- Enable phishing-resistant authentication for all privileged users in scope.
- Close residual findings under a two-person-rule change-control regime.

Phase 4: Full Deployment & Governance (Weeks 21-36)

- Migrate all business-critical applications onto the federated workload identity plane.
- Retire legacy stacks under a documented decommissioning doctrine.
- Establish quarterly control-owner committee reporting to Board Risk Committee.
- Independent assurance over the control environment; publish attestation.

11. Conclusion — From Compliance to Competitive Advantage

Static cloud secrets are obsolete. VAULT engineers workload identity as a universal, attested, ephemeral capability across AWS, Azure, and GCP — eliminating a class of breach by construction.

INSTITUTIONAL DOCTRINE SERIES

**Paper No. 07 of XXI — Zero-Secret Architectures
Governed by the Institutional Doctrine Series**

About the Author



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP | MBA | BEng

Mr. Upadrasta has over 27 years' experience in business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management. His career spans all four major consulting firms — Deloitte, PwC, EY and KPMG — with 21 years dedicated to financial services and banking. He has worked with the largest global corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI and SAS70.

Professional Memberships, Organisations & Associations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing — Schiphol University
- Honorary Senior Lecturer — Imperials
- Researcher — University College London (UCL)
- Lead Auditor — ISF Auditors and Control
- Platinum Member — Information Systems Audit and Control Association (ISACA), London Chapter
- Gold Member — International Information Systems Security Certification Consortium (ISC)²®, London Chapter
- Cyber Security Programme Lead — Professional Risk Management International Association (PRMIA)

Contact: info@kieranupadrasta.com · www.kie.ie · linkedin.com/in/kieranupadrasta

References

Primary Regulatory Sources

- Regulation (EU) 2022/2554 (DORA), EUR-Lex
- Regulation (EU) 2024/1689 (EU AI Act), EUR-Lex
- Directive (EU) 2022/2555 (NIS2), EUR-Lex
- Regulation (EU) 2024/1183 (eIDAS 2.0 / EUDI Wallet), EUR-Lex
- Bank of England PS6/21 and SS1/21 — Operational Resilience of Important Business Services
- FCA PS21/3 — Building Operational Resilience
- Proposed PSD3 / PSR (COM(2023) 367 / 368 final)
- SEC 17 CFR §229.106 — Cybersecurity Disclosure Rule
- 12 CFR Part 30 App. D — OCC Heightened Standards
- FFIEC Authentication & Access to Financial Institution Services (2021)

Standards and Frameworks

- ISO/IEC 42001:2023 — Artificial Intelligence Management Systems
- ISO/IEC 27001:2022 — Information Security Management Systems
- ISO/IEC 27701:2019 — Privacy Information Management
- NIST AI Risk Management Framework (AI RMF 1.0)
- NIST SP 800-207 — Zero Trust Architecture
- NIST SP 800-63-4 (Public Draft) — Digital Identity Guidelines
- NIST FIPS 140-3 — Cryptographic Module Validation
- NIST FIPS 203 / 204 / 205 — Post-Quantum Cryptography Standards (2024)
- OpenID Financial-grade API (FAPI) 2.0 Security Profile
- OAuth 2.0 PAR (RFC 9126), PKCE (RFC 7636), Token Exchange (RFC 8693), DPoP (RFC 9449)
- SAML 2.0 Core and Profiles (OASIS)
- SCIM 2.0 (RFC 7643 / 7644)
- OWASP ASVS v4.0 and OWASP API Security Top 10
- MITRE ATT&CK and MITRE ATLAS for AI

Industry Research & Technical Documentation

- PingIdentity — PingFederate 12.x Administrative Guide
- PingIdentity — PingOne Protect Risk Engine Whitepaper (2025)
- CISA Zero Trust Maturity Model v2.0
- NCSC Cloud Security Principles and Identity & Authentication Guidance
- ENISA — Threat Landscape for AI (2025)
- Gartner — Access Management Magic Quadrant (2025)
- Forrester — The State of Phishing-Resistant Authentication (2025)
- PRA SS2/21 — Outsourcing and Third-Party Risk Management
- EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04)

- DORA RTS on Threat-Led Penetration Testing (Commission Delegated Regulation)

© 2026 Kieran Upadrasta. All rights reserved. This document is governed by the Institutional Doctrine Series copyright framework.