

EVENT-DRIVEN IDENTITY

SCIM, PingIDM and the Real-Time Synchronisation Doctrine for Hybrid and Multi-Cloud Banking Estates

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 · 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

Turn identity synchronisation into a real-time event doctrine across every hybrid and multi-cloud banking estate — reportable at board level, replayable for any regulator.
< 15s Propagation SLO | 99.999% Event Bus Availability | Zero Batch Drift | Hourly Reconciliation

The event-driven identity is no longer a technical choice — it is a board-level governance decision. Turn identity synchronisation into a real-time event doctrine across every hybrid and multi-cloud banking estate — reportable at board level, replayable for any regulator.

KEY FINDING — THE PULSE FRAMEWORK

PULSE eliminates batch-identity staleness as an attack surface. Every attribute change propagates in seconds, not hours, and leaves a regulator-grade evidence trail from publisher to downstream.

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Event-Driven Identity 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 — Engineering Event-Driven Identity

Event-driven identity is the only architecture that keeps pace with cloud-scale attribute change. Batch is a regulatory finding waiting to be written.

3.1 Event Bus Architecture

- Kafka cluster with tiered storage and 72h hot retention.
- Topic-per-domain with compacted history for current-state views.
- Consumer groups for each downstream integration.
- Schema registry with semantic versioning and deprecation.

3.2 SCIM 2.0 at Scale

- PATCH-based updates avoid full-attribute overwrites.
- Rate-limit envelope sized for peak joiner/leaver bursts.
- Parallel provisioning with idempotency keys.
- Backpressure signals honoured by upstream publishers.

3.3 Reconciliation & Drift

- Hourly reconciliation compares source of truth to downstream state.
- Drift alerts tagged with attribute and downstream system.
- Automated remediation for a catalogued set of drift classes.
- Board-visible drift percentage as a compliance KPI.

3.4 Observability & Forensics

- Every event tagged with trace-id for end-to-end replay.
- OpenTelemetry spans across producer, bus, consumer.
- Cryptographic attestation of critical attribute changes.
- 7-year evidence retention per OCC/FFIEC.

4. The PULSE Framework — Provisioning · Unified · Live-sync · SCIM-native · Event-driven

PULSE converts batch identity provisioning into a real-time event-driven doctrine. Each dimension eliminates staleness as an attack surface.

4.1 P — Provisioning-as-an-Event

- Every identity change is a first-class business event.
- Event ordering guaranteed via Kafka / EventBridge with causal IDs.
- Dead-letter and replay queues instrumented and alertable.
- Publisher/subscriber contracts versioned and tested.

4.2 U — Unified Schema

- SCIM 2.0 + custom extensions as the canonical schema.
- Schema registry with backward-compat enforcement.
- No vendor-specific JSON shapes crossing service boundaries.
- Attribute deprecation calendar published.

4.3 L — Live-sync Guarantees

- End-to-end propagation SLO < 15 seconds for critical attributes.
- Freshness monitored per downstream, per attribute.
- Reconciliation job catches any drift within the hour.
- Emergency full-resync runbook rehearsed quarterly.

4.4 S — SCIM 2.0 Native

- All provisioning via RFC 7643 / 7644.
- Patch semantics, not replace, for attribute updates.
- HTTP 2 / gRPC for high-volume provisioning.
- SCIM filter language enforced at the gateway.

4.5 E — Event-Driven Compensations

- Failed provisions compensated via event-sourced workflows.
- Saga pattern for multi-target provisioning.
- Audit events for every success and failure.
- Exactly-once semantics for critical provisioning actions.

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 event-driven identity provisioning.
DORA	Art. 9 (Protection)	Continuous ICT protection including identity, access, and cryptographic controls.	Framework in §4 engineers event-driven identity provisioning 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 event-driven identity provisioning incidents.
NIS2	Art. 21	Risk-management measures including MFA, access control, and cryptography.	Phishing-resistant authentication + cryptographic trust bound to event-driven identity provisioning.
EU AI Act	Annex III §5(b)	High-risk AI in access / underwriting / fraud — includes adaptive identity models.	Any AI model involved in event-driven identity provisioning 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 event-driven identity provisioning.
NIST AI RMF	GOVERN + MEASURE	Govern AI risk with measurable, testable outcomes tied to business objectives.	Board-level KPIs in §7 tied to event-driven identity provisioning.
NIST SP 800-207	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to event-driven identity provisioning.

6. Board-Level Governance

Identity staleness is an exploitable attack surface. Board accountability under DORA Art. 9 requires real-time provisioning.

6.1 Essential Board Questions

- What is our end-to-end propagation SLO for an attribute change, and are we inside it?
- How often does drift occur between source of truth and downstream systems?
- What is our reconciliation cadence, and how are drift exceptions actioned?
- Do we have an exactly-once guarantee for critical provisioning actions?
- Can we replay any provisioning event in the last 7 years?
- What is our concentration risk on the event bus and its vendor?

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.
- Stale entitlements in a DORA-scoped system are themselves an 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
Propagation p99 latency	< 15 s	Internal SLO
Event bus availability	99.999%	DORA Art. 11
Reconciliation cadence	Hourly	Internal runbook
Drift exceptions per day	< 10 across Tier-1	Compliance KPI
SCIM PATCH adoption	100% of updates	Architecture review

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
Batch identity jobs remaining	0 (Tier-1)	DORA Art. 9
Stale role exposures > 1 hour	0	Internal audit
Dead-letter queue backlog	0 at day-end	SRE SLO
Event-bus vendor concentration	< 50%	PRA SS2/21
Mean time to revoke	< 60 s	NIST SP 800-207

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
DORA Art. 9 control test pass rate	100%	DORA RTS
SCIM 2.0 conformance	Certified	RFC 7643/7644
Evidence retention	7 years	OCC/FFIEC
NIS2 24-h early-warning	100%	NIS2
ISO/IEC 27001 audit findings	Zero majors	ISO 27001

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 Converting a 24-hour batch to a 15-second PULSE

SECTOR: Tier-1 European Bank

Converting a 24-hour batch to a 15-second PULSE

Challenge — Nightly provisioning batch caused up to 24-hour staleness; two regulatory findings on orphaned accounts; annual breach risk.

Solution — Introduced PULSE: Kafka event bus, SCIM 2.0 native, hourly reconciliation, board KPI.

Outcome — Propagation p99 now 11 s; orphan accounts eliminated; supervisory findings closed.

8.2 Live SCIM sync across AWS, Azure, and on-prem

SECTOR: Global Custodian — Cloud Migration

Live SCIM sync across AWS, Azure, and on-prem

Challenge — Migration to multi-cloud left identity in three places with divergent state; audit could not reconcile entitlements.

Solution — PULSE event bus as source of truth; SCIM connectors on every cloud IdP; drift alerts.

Outcome — State reconciled within 9 weeks; audit finding closed; cloud migration unblocked.

8.3 Day-zero provisioning and instant leaver revocation

SECTOR: Payment Provider — Joiner/Leaver Automation

Day-zero provisioning and instant leaver revocation

Challenge — Leavers retained access up to 48 hours; P1 incident after ex-employee exfiltrated data.

Solution — PULSE event-sourced joiner/leaver flow; leaver revocation within 30 seconds; mandatory evidence attestation.

Outcome — Leaver mean-time-to-revoke fell from 48 h to 24 s; P1 incident root cause addressed.

11. Conclusion — From Compliance to Competitive Advantage

Identity staleness is an attack surface. PULSE converts provisioning from a batch utility into a real-time control plane — reported at board level, replayable for regulators, and aligned to every major ICT-risk regulation.

INSTITUTIONAL DOCTRINE SERIES

**Paper No. 04 of XXI — Event-Driven Identity
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.