

# THE INTEGRATION FACTORY

## A Java Adapter Framework for Industrial-Scale Identity Onboarding of SWIFT, Murex and Trading Platforms — A Doctrine for Repeatable Federation

*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 ISC<sup>2</sup> · PRMIA Cyber Programme Lead

---

[www.kie.ie](http://www.kie.ie) · [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [linkedin.com/in/kieranupadrasta](https://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**

**Convert identity onboarding from artisanal projects into an industrial factory. One adapter SDK, one certified registry, one evidence chain — applied to every regulated trading platform in the estate.**

**> 3 Systems Onboarded / Sprint | Zero Bespoke Adapters | 100% Conformance | Industrial Repeatability**

The the integration factory is no longer a technical choice — it is a board-level governance decision. Convert identity onboarding from artisanal projects into an industrial factory. One adapter SDK, one certified registry, one evidence chain — applied to every regulated trading platform in the estate.

### **KEY FINDING — THE ANVIL FRAMEWORK**

ANVIL abolishes bespoke integrations. Every trading system is onboarded as a standards-based identity consumer through a certified adapter with regulator-grade evidence. Cycle times collapse; compliance improves; supervisory findings drop.

## 2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. The Integration Factory 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 — The Adapter Factory

The onboarding of trading systems is often the slowest phase of a federation programme — not because the technology is hard, but because the organisation treats each system as a bespoke project. ANVIL turns onboarding into an industrial process.

### 3.1 The Java Adapter SDK

- Shared codebase with JWT, SAML, and OAuth core primitives.
- Adapters inherit standards conformance by construction.
- Hot-reload of adapter configuration without identity-plane restart.
- Integration test harness runs against live PingFederate test cluster.

### 3.2 SWIFT CSP Integration Pattern

- mTLS sender-constrained tokens aligned to SWIFT Customer Security Programme.
- Dual-signature workflow for high-value payment instructions.
- OCSP stapling for SWIFT certificate chain validation.
- Attestation produced for every SWIFT onboarding.

### 3.3 Murex / Calypso Onboarding Blueprint

- Role-to-entitlement mapping captured in Git; no bespoke DB tables.
- Segregation-of-duties (SoD) checks enforced at token issuance.
- End-of-day reconciliation between entitlements and positions.
- Regulatory reporting (EMIR, MiFID II) joined via identity metadata.

### 3.4 Continuous Conformance & Certification

- OIDC conformance suite run in CI for every adapter PR.
- FAPI 2.0 profile certified annually by an accredited lab.
- Deprecation calendar enforced via API gateway policy.
- Cycle-time and throughput reported quarterly to the board.

## 4. The ANVIL Framework — Adapters · Native · Verifiable · Industrial · Lifecycle

ANVIL operationalises the onboarding of regulated trading systems — SWIFT, Murex, Calypso, Bloomberg, Refinitiv — to a Tier-0 federation plane. Each dimension is engineered for industrial repeatability, not artisanal one-offs.

### 4.1 A — Adapter Factory

- Shared Java SDK with standards-conformant OIDC, SAML, OAuth 2.0 adapters.
- Certified adapter registry; no bespoke integrations in production.
- Versioned adapter SLOs with independent test harness.
- Continuous conformance testing against OpenID + OAuth conformance suites.

### 4.2 N — Native Integration Patterns

- SWIFT CSP-compliant federation with mTLS sender-constrained tokens.
- Murex FO/BO workflows integrated via OIDC with DPoP-bound tokens.
- Bloomberg / Refinitiv market-data systems consumed via workload identity.
- Trading platforms onboarded as standards-based identity consumers, not SSO targets.

### 4.3 V — Verifiable Onboarding

- Each onboarding produces a signed evidence package.
- Attestation linked to change ticket and architecture review approval.
- Rollback runbook rehearsed pre-go-live.
- Regulator-grade audit trail from design to production.

### 4.4 I — Industrial Repeatability

- Go-live cadence: > 3 systems / sprint at steady state.
- Standardised deployment blueprint for new adapters.
- Documentation-as-code: every adapter publishes a machine-readable spec.
- Continuous improvement loop measured in cycle time.

### 4.5 L — Lifecycle Governance

- Adapter deprecation calendar published 18 months in advance.
- Decommissioning doctrine for sunset systems.
- Contract-test regression suite blocks breaking changes.
- Ownership map signed off by the Identity Risk Committee.

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

Regulation	Article / Control	Obligation	Paper Response
<b>NIST SP 800-207</b>	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to identity onboarding of regulated trading systems.

## 6. Board-Level Governance

The onboarding velocity of regulated systems is a leading indicator of operational-resilience maturity. Slow onboarding = technical debt the regulator sees.

### 6.1 Essential Board Questions

- How many bespoke (non-standard) identity integrations remain in production?
- What is our average cycle time from request to production go-live for a new system?
- Do we certify every adapter against OpenID / OAuth conformance suites?
- Is our adapter deprecation calendar published and enforced?
- Can we produce a signed onboarding evidence package for every regulated system?
- What is our plan to migrate legacy custom integrations onto the Adapter Factory?

### 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.
- Bespoke adapters accumulate as shadow ICT; a DORA Art. 8 asset-inventory gap.

## 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
Systems onboarded per sprint	> 3	Internal throughput
Mean onboarding cycle time	< 14 days	DORA Art. 9 agility
Adapter conformance test pass rate	100%	OIDC conformance
Bespoke adapters in production	0 (Tier-1)	Asset register
Adapter release cadence	≥ Monthly	Engineering excellence

### 7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
Static-secret usage in adapters	0	NIST SP 800-207
Unpatched adapter deprecations	0	Deprecation calendar
Adapter test coverage	≥ 90%	OWASP ASVS
Contract-test regression rate	< 1% per release	Engineering SLO
Shadow-ICT integration count	0	DORA Art. 8

### 7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
FAPI 2.0 certification status	Current	OpenID FAPI
SWIFT CSP attestation	Current	SWIFT CSCF
DORA ICT asset inventory accuracy	100%	DORA Art. 8
Evidence package completeness	100%	Internal audit
Annual penetration test on adapter SDK	Passed	DORA RTS

## 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 SWIFT, Murex, and Calypso onboarded through ANVIL in 10 months

**SECTOR:** Tier-1 Global Bank — 180 trading platforms

#### SWIFT, Murex, and Calypso onboarded through ANVIL in 10 months

**Challenge** — 140+ bespoke integrations for trading systems; 45-day average cycle time; inconsistent SoD enforcement; SWIFT CSP audit findings outstanding.

**Solution** — Introduced ANVIL adapter factory; certified SDK; phased migration of 180 platforms; dual-signature SWIFT workflow; SoD enforced at token issuance.

**Outcome** — Cycle time reduced from 45 to 11 days; SWIFT CSP findings closed; 94% of integrations migrated to certified adapters; £18M annual operational saving.

### 8.2 Murex onboarded under ANVIL with SoD-at-token

**SECTOR:** Investment Bank — Fixed Income Platform

#### Murex onboarded under ANVIL with SoD-at-token

**Challenge** — Murex had 1,600 role-to-entitlement combinations managed manually; SoD violations discovered during internal audit; no automated reconciliation.

**Solution** — ANVIL adapter extracted role map to Git; SoD checks enforced at token issuance; daily reconciliation with trading book; evidence chain for every issuance.

**Outcome** — SoD violations eliminated; audit finding closed; regulatory reporting accuracy improved; cost of controls reduced by £3.2M annually.

### 8.3 Bloomberg and Refinitiv onboarded as workload identities

**SECTOR:** Global Asset Manager — Market Data Platforms

#### Bloomberg and Refinitiv onboarded as workload identities

**Challenge** — Market data systems consumed static API keys held by individuals; revocation was manual; OCC finding on segregation.

**Solution** — Workload identity for all market-data consumers via SPIFFE/SPIRE; ephemeral credentials; ANVIL certified adapter for vendor APIs.

**Outcome** — Static keys eliminated; revocation time < 60s; OCC finding closed; vendor-risk rating improved two grades.

## 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 identity onboarding of regulated trading systems 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 identity onboarding of regulated trading systems.
- Count bespoke adapters in the target; any > 10% of total is a red flag for post-deal integration cost.

### 9.3 Valuation Impact Scenarios

- **Scenario A — Concentration Risk:** target relies on a single vendor for 90%+ of identity onboarding of regulated trading systems. Valuation haircut of 4-6% of EBITDA multiple to fund redesign.
- **Scenario B — Undocumented AI in identity onboarding of regulated trading systems:** 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 identity onboarding of regulated trading systems 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 identity onboarding of regulated trading systems: systems, vendors, cryptographic dependencies.
- Baseline current KPIs — latency, availability, coverage, exposure.
- DORA Art. 9 gap analysis and regulatory-obligation-to-control map for identity onboarding of regulated trading systems.
- Board briefing: impact tolerances, concentration risk, liability framing.

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

- Target topology for identity onboarding of regulated trading systems 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 identity onboarding of regulated trading systems 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 identity onboarding of regulated trading systems 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

Identity onboarding is either an industrial capability or an accumulating tax on the bank's ability to innovate. ANVIL removes the choice. Every regulated trading system becomes a standards-based identity consumer through a certified adapter — predictable, repeatable, and defensible. Cycle times collapse; audit findings drop; engineering capacity is freed for strategic work. The Adapter Factory is the governance model the board deserves.

### **INSTITUTIONAL DOCTRINE SERIES**

**Paper No. 03 of XXI — The Integration Factory  
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)<sup>2</sup>®, London Chapter
- Cyber Security Programme Lead — Professional Risk Management International Association (PRMIA)

---

**Contact:** [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie) · [linkedin.com/in/kieranupadrasta](https://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.