

IDENTITY AS THE PRIMARY ENFORCEMENT LAYER

Unifying Endpoint, Network and Access Decisioning — A Doctrine for Policy Singularity Across the Security Stack

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

Engineer identity as the single, authoritative enforcement layer across endpoint, network, and application planes.

**Singular Policy Vocabulary | Cross-Layer Identity Context | Continuous Verification
| Unified Evidence Chain**

The identity as the primary enforcement layer is no longer a technical choice — it is a board-level governance decision. Engineer identity as the single, authoritative enforcement layer across endpoint, network, and application planes.

KEY FINDING — THE AEGIS FRAMEWORK

AEGIS collapses the security stack into a single identity-centric control plane. Duplicate enforcement disappears; gaps close; investigation time drops.

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Identity as the Primary Enforcement Layer 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 — Identity as the Enforcement Layer

The security stack collapses when identity becomes the primary enforcement layer. AEGIS engineers that collapse deliberately, not accidentally.

3.1 Endpoint-Identity Integration

- Device posture enforced at authentication.
- Continuous trust evaluation via endpoint telemetry.
- Token binding to device via hardware attestation.
- Identity-driven endpoint isolation.

3.2 Network-Identity Integration

- Identity-aware proxy for all access.
- Microsegmentation tied to identity claims.
- NAC decisions informed by identity posture.
- DNS and edge policies identity-contextualised.

3.3 Application-Identity Integration

- All access brokered through the federation plane.
- ABAC per request via HELIX PDP.
- Cryptographic evidence per decision.
- Legacy apps onboarded via ANVIL adapters.

3.4 Unified Observability

- Endpoint, network, app events tagged with identity context.
- Cross-layer correlation in SIEM.
- UEBA across all three layers.
- Board dashboard: cross-layer enforcement health.

4. The AEGIS Framework — Access · Enforcement · Governance · Identity · Singular

AEGIS engineers identity as the primary enforcement layer — the single, authoritative surface where access decisions are made across endpoint, network, and application planes.

4.1 A — Access as the Primary Control

- Identity decisions gate every endpoint, network, and app action.
- Zero Trust per NIST SP 800-207 — continuous verification.
- Phishing-resistant authentication prerequisite for sensitive actions.
- Device posture bound to identity.

4.2 E — Enforcement Everywhere

- Endpoint agents enforce identity-derived policy.
- Network segmentation tied to identity context.
- Application-layer access brokered through the control plane.
- Cloud workload access governed identically.

4.3 G — Governance Across Layers

- Unified policy language across identity, network, endpoint.
- Single audit trail for cross-layer decisions.
- Board dashboard shows cross-layer enforcement health.
- Change control integrated with FABRIC.

4.4 I — Identity-Centric Observability

- Every access event tagged with identity context.
- Cross-layer correlation via OpenTelemetry.
- SIEM ingestion aligned to MITRE ATT&CK identity techniques.
- UEBA baselines per identity across layers.

4.5 S — Singular Policy Vocabulary

- One canonical claim vocabulary across all layers.
- Policy-as-code in Git for all enforcement points.
- No divergent policy between endpoint, network, app.
- Architecture review board owns the schema.

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 identity as the primary enforcement layer.
DORA	Art. 9 (Protection)	Continuous ICT protection including identity, access, and cryptographic controls.	Framework in §4 engineers identity as the primary enforcement layer 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 identity as the primary enforcement layer incidents.
NIS2	Art. 21	Risk-management measures including MFA, access control, and cryptography.	Phishing-resistant authentication + cryptographic trust bound to identity as the primary enforcement layer.
EU AI Act	Annex III §5(b)	High-risk AI in access / underwriting / fraud — includes adaptive identity models.	Any AI model involved in identity as the primary enforcement layer 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 identity as the primary enforcement layer.
NIST AI RMF	GOVERN + MEASURE	Govern AI risk with measurable, testable outcomes tied to business objectives.	Board-level KPIs in §7 tied to identity as the primary enforcement layer.

Regulation	Article / Control	Obligation	Paper Response
NIST SP 800-207	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to identity as the primary enforcement layer.

6. Board-Level Governance

Fragmented enforcement across endpoint, network, and application planes creates gaps. AEGIS unifies them under identity.

6.1 Essential Board Questions

- Is our policy vocabulary consistent across endpoint, network, and application layers?
- Do we correlate events cross-layer in SIEM under a single identity key?
- Is device posture bound to identity at token issuance?
- Can we produce a unified audit trail for any access decision?
- Are legacy apps onboarded via certified adapters to the control plane?
- Do we run UEBA across all three layers under a single identity baseline?

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.
- Fragmented enforcement is a leading root cause of detection gaps in post-incident investigations.

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
Cross-layer enforcement coverage	100% (Tier-1)	AEGIS
Cross-layer correlation latency	< 1 min	SIEM SLO
UEBA baseline coverage	100% privileged identities	Internal
p99 access decision latency	< 90 ms	Internal SLO
Device posture at token issuance	100%	CISA ZTMM

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
Policy divergence across layers	0	Governance
Shadow enforcement points	0 (Tier-1)	Asset register
Legacy apps outside control plane	< 5%	SUNSET
Cross-layer blind spots	0	SIEM
UEBA alerts actioned	< 15 min	SOC SLO

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
NIST SP 800-207 Zero-Trust alignment	Advanced	NIST
CISA ZTMM v2.0	Advanced+	CISA
DORA Art. 9 test pass rate	100%	DORA RTS
ISO/IEC 27001 audit	Zero majors	ISO
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 Unifying endpoint, network, and app under AEGIS

SECTOR: Tier-1 Bank — Zero Trust Programme

Unifying endpoint, network, and app under AEGIS

Challenge — Fragmented enforcement across 3 layers; SIEM correlation required manual pivots; audit finding on detection gaps.

Solution — AEGIS: identity-aware proxy; ABAC at app layer; endpoint posture at token issuance.

Outcome — Cross-layer correlation automated; audit finding closed; investigation time fell from 6 h to 32 min mean.

8.2 Identity-aware microsegmentation

SECTOR: Investment Bank — Privileged Network Paths

Identity-aware microsegmentation

Challenge — Privileged network paths defined by IP ranges; audit finding on segmentation-to-identity traceability.

Solution — AEGIS: microsegmentation policy expressed as identity claims.

Outcome — Audit finding closed; privileged-path traceability complete; insurance premium fell 6%.

8.3 Device posture bound to identity

SECTOR: Insurance Group — Endpoint Trust

Device posture bound to identity

Challenge — Endpoint posture signals not integrated into authentication; two near-miss incidents from compromised devices with valid tokens.

Solution — AEGIS: device attestation at token issuance; continuous trust evaluation.

Outcome — Near-miss root cause addressed; compromised-device token issuance prevented.

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 as the primary enforcement layer 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 as the primary enforcement layer.
- Check policy vocabulary consistency across layers in the target.

9.3 Valuation Impact Scenarios

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

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

- Target topology for identity as the primary enforcement layer 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 as the primary enforcement layer 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 as the primary enforcement layer 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

Security-stack fragmentation creates detection gaps and investigation lag. AEGIS unifies enforcement under identity — a single authoritative surface across endpoint, network, and application planes.

INSTITUTIONAL DOCTRINE SERIES

**Paper No. 15 of XXI — Identity as the Primary Enforcement Layer
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.