BEYOND RBAC

Attribute-Driven Authorisation for Cloud-Scale Financial Data Systems — A Doctrine for Dynamic Entitlement at Petabyte Scale

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 attribute-based authorisation for petabyte-scale financial data systems — fine-grained, queryable, and regulator-ready.

< 5 ms p99 ABAC Decisions | Petabyte-Scale Coverage | Reverse-Mapped Policy | Deny-by-Default Posture

The beyond rbac is no longer a technical choice — it is a board-level governance decision. Engineer attribute-based authorisation for petabyte-scale financial data systems — fine-grained, queryable, and regulator-ready.

KEY FINDING — THE QUARK FRAMEWORK

QUARK replaces RBAC with ABAC at cloud-scale. Policy becomes queryable, data-lineage-aware, and auditable in ways RBAC never could be.

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Beyond RBAC 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 — ABAC at Petabyte Scale

RBAC fails at cloud-scale data systems. Attribute-based authorisation is the only viable model — but only when engineered correctly.

3.1 ABAC Decision Model

- NIST SP 800-162 Four Elements: subject, object, action, environment.
- Rego/Cedar policies at the data-gateway layer.
- Obligation patterns supported (XACML alignment).
- Deny-by-default; reason codes propagated upstream.

3.2 Attribute Provenance & Freshness

- Single canonical attribute schema.
- Provenance metadata per attribute value.
- Freshness SLO per attribute class.
- Attribute revocation propagates via event bus in < 15 s.

3.3 Data-Lineage + Entitlement Graph

- Graph of data assets, owners, classifications, and consumers.
- Policy reasoning over the graph.
- Sensitive-data discovery automated.
- Regulatory reporting queries over the graph.

3.4 Scale Engineering

- PDP co-located with data gateway for p99 < 5 ms.
- Deterministic decision caching with short TTLs.
- Horizontal scaling; no single choke point.
- Decision-throughput 30M+ per day per domain.

© 2026 Kie Sanhedrai

4. The QUARK Framework — Queryable · Unified · Attribute · Runtime · Knowledge

QUARK engineers attribute-based authorisation for petabyte-scale data systems. Fine-grained, queryable, and auditable.

4.1 Q — Queryable Policy

- Policy expressed as code and queryable at design time.
- Reverse-mapping: who can access what.
- Impact analysis automated for policy changes.
- Policy queries integrated with ticketing and approvals.

4.2 U — Unified Attribute Sources

- Single schema for attributes across systems.
- Provenance preserved per attribute.
- Freshness SLO per attribute type.
- No duplicate attribute stores.

4.3 A — Attribute-Driven Decisions

- Decisions based on identity, resource, action, and context attributes.
- NIST SP 800-162 ABAC model as the reference.
- Obligation-pattern support (XACML-style).
- Purpose-limitation enforced via attribute.

4.4 R — Runtime Enforcement

- PDP embedded at petabyte-scale data gateways.
- Sub-5 ms decision latency budget.
- Deny-by-default posture.
- Caching with short TTLs to balance freshness and latency.

4.5 K — Knowledge-Graph Integration

- Organisation's data lineage + entitlement graph.
- Policy reasoning over the knowledge graph.
- Data classification and sensitivity tagged at source.
- Regulatory reporting aligned to graph attributes.

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

6. Board-Level Governance

RBAC fails at cloud-scale data systems. The regulatory expectation in 2026 is fine-grained, attribute-based authorisation.

6.1 Essential Board Questions

- Do we have fine-grained ABAC on our cloud-scale data gateways?
- Can we produce a reverse map: 'who can access this data set'?
- Is attribute freshness SLO'd per attribute class?
- Do we enforce deny-by-default on every data gateway?
- Is our data-lineage and entitlement graph integrated with policy reasoning?
- Do we run policy impact analysis before every change?

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.
- GDPR Art. 5 purpose-limitation is enforced technically, not policy-only; failure to do so is an Art. 83 fine line item.

©2026 Kieran Sandhu. www.kie.ie

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
ABAC decision p99	**< 5 ms**	Engineering SLO
Data-gateway coverage	**100% (Tier-1)**	QUARK
Attribute freshness	**< 15 s revocation**	Internal SLO
Policy release cadence	**Weekly**	Engineering
Reverse-map query time	**< 60 s**	Engineering

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
RBAC-only authorisation on Tier-1 data	**0**	QUARK
Undocumented access paths	**0**	Graph coverage
Overpermissioned entitlements	**< 2%**	Access review
Sensitive-data exposure (HDPR index)	**Baseline – 30%**	Governance
Purpose-limitation violations	**0**	GDPR Art. 5

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
GDPR Art. 5 purpose-limitation proof	**Attested**	GDPR
DORA Art. 9 test pass rate	**100%**	DORA RTS
NIST SP 800-162 alignment	**Reference**	NIST
Evidence retention	**7 years**	OCC/FFIEC
ISO 27001 audit	**Zero majors**	ISO

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 ABAC enforcement on 4 PB of regulated data

SECTOR: Global Bank — Data Lake at Petabyte Scale

ABAC enforcement on 4 PB of regulated data

Challenge — RBAC could not express purpose-limitation; GDPR supervisory finding; data consumers could pull beyond approved scope.

Solution — QUARK: ABAC at data gateway; data-lineage graph; deny-by-default.

Outcome — Supervisory finding closed; sensitive-data exposure index down 38%; policy queries power quarterly regulatory reporting.

8.2 Fine-grained consent enforcement

SECTOR: Wealth Platform — Client Data

Fine-grained consent enforcement

Challenge — Client data access used broad roles; audit finding on consent enforcement at the data layer.

Solution — QUARK: attribute-driven consent checks at every read; evidence chain.

Outcome — Audit finding closed; customer trust NPS up 9 points.

8.3 Purpose-limitation for analytics queries

SECTOR: Insurance Group — Underwriting Analytics

Purpose-limitation for analytics queries

Challenge — Analytics queries accessed underwriting data without purpose check; GDPR exposure.

Solution — QUARK: purpose-attribute enforced on every query; obligation patterns.

Outcome — Purpose-limitation enforced technically; GDPR posture improved; legal team reduced manual review by 60%.

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 attribute-driven authorisation 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 attribute-driven authorisation.
- Assess the target's data-authorisation model; RBAC-only on cloud-scale data is a finding.

9.3 Valuation Impact Scenarios

- **Scenario A — Concentration Risk**: target relies on a single vendor for 90%+ of attribute-driven authorisation. Valuation haircut of 4-6% of EBITDA multiple to fund redesign.
- **Scenario B — Undocumented AI in attribute-driven authorisation**: 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 attribute-driven authorisation onto its own estate; £8-14M one-off cost, £18-24M annual run-rate synergy.

© 2026 Kie Systems Ltd. www.kie.ie

10. Implementation Roadmap

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

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

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

- Target topology for attribute-driven authorisation 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 attribute-driven authorisation 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 attribute-driven authorisation 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.

© 2026 Kieran Upadrasta. www.kie.ie

11. Conclusion — From Compliance to Competitive Advantage

RBAC is insufficient for cloud-scale financial data systems. QUARK engineers fine-grained, queryable, data-lineage-aware ABAC as the reference architecture for regulated data in 2026.

INSTITUTIONAL DOCTRINE SERIES

Paper No. 18 of XXI — Beyond RBAC

Governed by the Institutional Doctrine Series

© 2026 Kie Systems Ltd. www.kie.ie

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)

© 2026 Kie Systems Ltd. www.kie.ie

- 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.