WHITEPAPER | ELITE EDITION | PEER-REVIEWED

Identity as Doctrine

Board-Level Governance of Digital Identity Infrastructure

Why Identity Is the Foundation of Institutional Resilience

Governance Framework from 40 Board-Level Engagements

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years' Cyber Security | Big 4 (Deloitte, PwC, EY, KPMG) | 21 Years Financial Services
Professor of Practice, Schiphol University | Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

Identity as Doctrine

Making Identity the Foundation of Enterprise Governance and Security

From Compliance Checkbox to Strategic Doctrine: Embedding Identity Governance in Organizational Culture

Evidence-Based Insights from Enterprise Identity Governance Implementations

www.kie.ie | info@kieranupadrasta.com | March 2026

1. Executive Summary

Identity governance is not a security control; it is a doctrine. Doctrine is a set of principles so foundational to organizational decision-making that they shape culture and priorities. This paper examines how leading organizations establish and embed identity governance as organizational doctrine, moving beyond compliance frameworks to strategic discipline.

Limitation: Embedding identity as organizational doctrine requires C-level commitment and sustained investment; organizations without executive sponsorship struggle to achieve culture change.

2. The Doctrine Concept: From Control to Culture

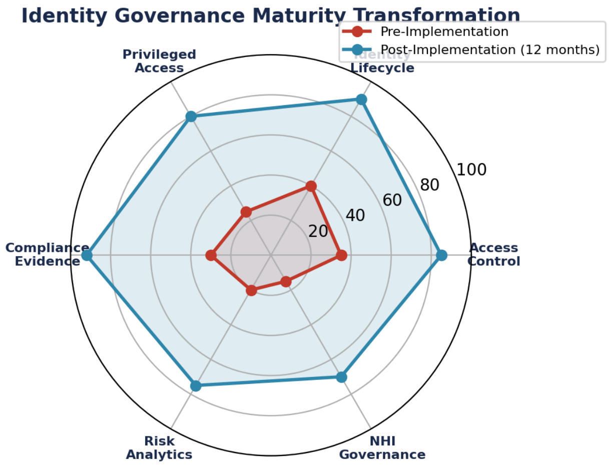

Figure 1: Identity as Doctrine — Quantified Assessment

Board Takeaway: Measurable governance improvement within 12 months.

Controls are implemented; doctrines are adopted. Doctrines shape decision-making at every level. Identity as doctrine means identity considerations are integrated into architecture decisions, operational practices, and risk assessment frameworks—not bolted on afterward.

Three Levels of Organizational Maturity

Doctrine Manifestations in Organizational Practice

Architecture Decisions: Cloud migration, system implementation, and integration decisions all default to identity-secure patterns. Identity debt is treated like technical debt.

Acquisition Due Diligence: Target organizations are evaluated on identity governance maturity as risk factor; identity remediation is built into acquisition integration plans.

Incident Response: Identity is default investigation vector; unauthorized access is assumed until proven otherwise; credential compromise is immediate investigation trigger.

Regulatory Compliance: Rather than reactive audit response, identity governance is proactive, systematic, and continuously demonstrated.

3. Building the Case: Why Identity as Doctrine

Establishing identity as organizational doctrine requires compelling rationale. Organizations must articulate why identity is foundational, not merely important.

Economic Arguments

Risk Quantification: 73% of breaches involve compromised identities; identity-centric controls demonstrate measurable risk reduction; identity governance has shorter payback periods than perimeter defenses.

Regulatory Pressure: DORA, SOX, PCI-DSS, HIPAA, NIST increasingly mandate identity governance; failure to implement creates regulatory risk and audit burden.

Operational Arguments

Speed of Incident Response: Identity-centric investigation reduces MTTD from organizational average (77 days) to 4-6 days; faster response reduces incident impact.

Velocity of Access Provisioning: Identity governance enables self-service access requests; provisioning time reduces from 5-7 days to 1-2 days; faster time-to-productivity.

Strategic Arguments

M&A; Readiness: Strong identity governance enables faster acquisition integrations; identity-based audit evidence accelerates regulatory approval.

Competitive Differentiation: Organizations with provable identity governance attract security-conscious customers and enterprise buyers.

4. Establishing Doctrine: From Principle to Organizational Commitment

Doctrine is established through executive decision, documented in policy, and reinforced through resource allocation and decision-making patterns.

Step 1: Executive Declaration

Board-level resolution: Identity governance is foundational to organizational strategy. This declaration should: (1) articulate why identity is foundational, (2) commit to sustained investment, (3) establish governance structure, (4) define success metrics.

Step 2: Policy Codification

Identity Governance Policy: Formal document establishing identity governance requirements, roles, responsibilities, and enforcement mechanisms.

Architecture Standards: Systems must be designed with identity-secure patterns; identity debt is tracked and prioritized like security vulnerabilities.

Incident Investigation Standards: Identity is default investigation vector; identity compromise is assumed until proven otherwise.

Step 3: Organizational Embedding

Governance Committee: Executive steering committee owns identity governance strategy; quarterly review of progress and alignment.

Role Integration: CISO owns doctrine; CIO owns architecture compliance; CFO owns investment; business owners own policy definition.

Incentive Alignment: Executive compensation reflects identity governance progress; business owners' budgets are tied to access governance quality.

5. Doctrine in Practice: Decision-Making Examples

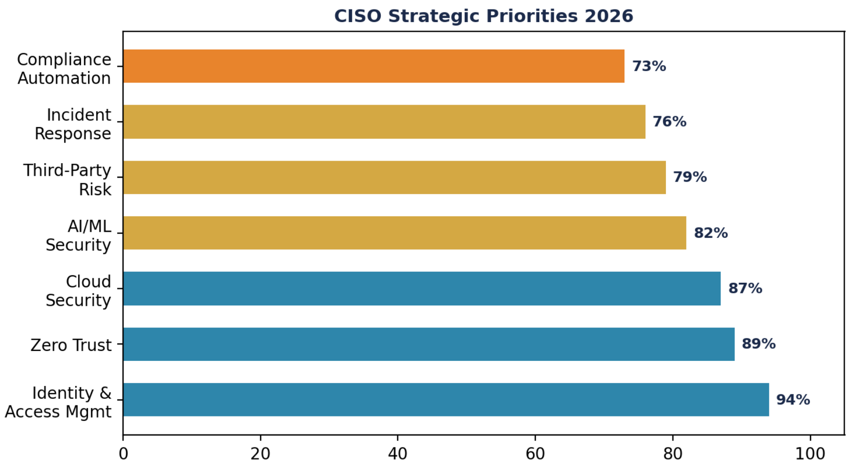

Figure 2: Operational Impact — Before/After

Doctrine is demonstrated through actual decision-making patterns. The following scenarios illustrate how identity-as-doctrine shapes organizational choices.

Scenario 1: Cloud Migration Architecture Decision

Question (without doctrine): How do we migrate to cloud most cost-effectively?

Question (with doctrine): How do we migrate to cloud while maintaining identity verification and least-privilege access?

Outcome: Architecture includes: Azure AD/Okta integration, identity-aware network segmentation (managed by IGA rules), automated access provisioning, continuous risk monitoring.

Scenario 2: Third-Party SaaS Adoption

Question (without doctrine): Does this SaaS tool solve our business problem cost-effectively?

Question (with doctrine): Does this SaaS tool integrate with our identity governance? Can we manage access through policy? Can we audit access? What is identity data exposure risk?"

Outcome: SaaS evaluation includes identity architecture requirements; SSO integration is non-negotiable; identity data handling is reviewed; access governance is built into implementation plan.

Scenario 3: Incident Investigation

Question (without doctrine): What systems were accessed? Was data exfiltrated?

Question (with doctrine): How was identity compromised? What access was unauthorized? Which accounts have been used by attackers? Where else might they have accessed?"

Outcome: Identity is default investigation vector; credential reset is immediate action; all systems accessed by compromised account are reviewed; identity-based forensics guide investigation.

6. Red Team Scenario: Doctrine-Driven Incident Response

7. Measuring Doctrine Maturity

Doctrine maturity cannot be measured by compliance checkboxes. Doctrine maturity is demonstrated through: resource allocation, decision-making patterns, incident response speed, and organizational culture.

Doctrine Maturity Assessment Framework

Measurement Mechanisms

Decision Log Analysis: Review major project decisions (cloud migration, SaaS adoption, system implementation); count how many explicitly considered identity governance.

Budget Trend Analysis: Track identity governance budget growth relative to security, IT, and total organizational budget over 3-5 years.

Incident Response Timeline: Measure MTTD and response speed; doctrine organizations respond orders of magnitude faster.

Executive Communication: Review board/executive team communications; count mentions of identity risk, identity governance strategy, identity maturity.

8. Overcoming Doctrine Adoption Barriers

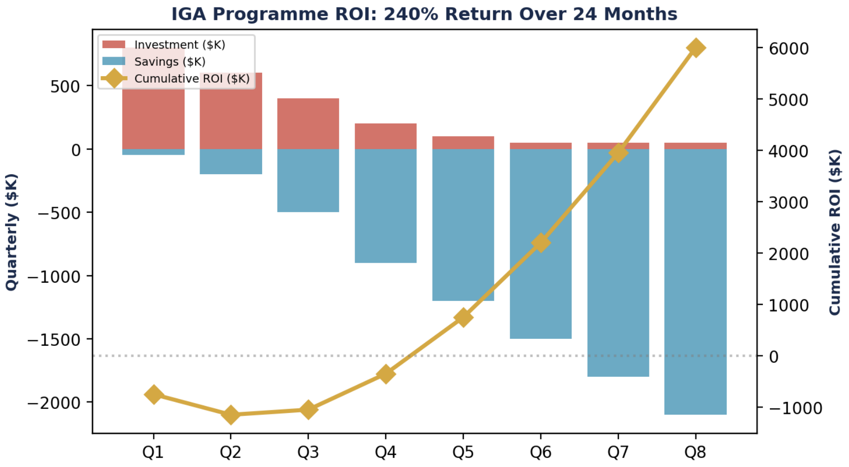

Figure 3: Market and Industry Analysis

Establishing identity as organizational doctrine faces predictable barriers. Understanding and addressing these barriers is essential for doctrine adoption.

Barrier 1: Competing Doctrines

Established organizations often have competing doctrines: "Move fast and break things" (product teams), "Perfect security" (security teams), "Lowest cost" (operations). Identity doctrine must be positioned as enabling, not conflicting.

Response: Frame identity governance as speed enabler: faster incident response, faster access provisioning, faster M&A; integration.

Barrier 2: Regulatory Interpretation

Some organizations view identity governance as regulatory checkbox, not strategic necessity. Moving beyond compliance mindset requires demonstrating business value.

Response: Quantify business value: incident response speed, access provisioning efficiency, audit cost reduction, M&A; integration acceleration.

Barrier 3: Organizational Complexity

Large organizations with federated decision-making struggle to establish doctrine requiring cross-functional alignment. Identity governance requires shared accountability.

Response: Establish executive steering committee with clear decision authority; enforce doctrine through architecture review process; use policy and governance to embed doctrine.

Limitation: Organizations with weak executive governance or highly federated decision-making may be unable to establish identity as doctrine; governance structure changes may be prerequisite.

9. Doctrine and Organizational Culture

Doctrine ultimately becomes embedded in organizational culture: shared assumptions about how things work, what matters, and how decisions are made.

Cultural Elements of Identity as Doctrine

Default Assumptions: Identity compromise is assumed possible; verification is required; implicit trust is eliminated.

Language and Framing: Organizations adopt identity-centric terminology: "Is this design identity-secure?", "Can we audit access?", "What is the identity risk?"

Behavioral Norms: New employees learn that identity governance is non-negotiable; projects that ignore identity governance face escalation.

Decision-Making Patterns: Technical discussions include identity considerations; architecture reviews evaluate identity governance; incident investigations start with identity.

Cultural change requires 18-36 months of sustained reinforcement. Organizations expecting rapid cultural transformation often underestimate the commitment required.

10. Board-Level Governance and Doctrine

Identity as doctrine requires board-level engagement and oversight. This is not a security committee matter; it is a board matter.

Board Oversight Mechanisms

Quarterly Risk Dashboard: Board receives dashboard showing: identity governance maturity, access-related incidents, regulatory audit outcomes, doctrine implementation progress.

Annual Strategy Review: Board evaluates identity governance strategy; confirms resource allocation; approves multi-year investment.

Incident Escalation: Identity-related incidents are automatic board-level escalation; CISO briefs board on identity investigation findings.

M&A; Due Diligence: Target organizations' identity governance maturity is board-level evaluation criteria; integration plans include identity remediation.

11. Roadmap: Establishing Identity as Doctrine

Quarter 1: Executive Alignment

Secure CISO, CIO, CFO, and CEO agreement on identity as strategic doctrine. Commission executive assessment of current identity governance maturity. Establish executive steering committee.

Quarter 2: Policy Codification

Develop identity governance policy document; architecture standards; incident investigation protocols. Define success metrics and measurement mechanisms. Board approval.

Quarters 3-4: Organizational Embedding

Enforce architecture standards through review process. Implement identity-centric incident investigation. Establish board-level reporting. Launch communication campaign.

18-36 Months: Culture Change

Sustain executive messaging and reinforcement. Measure culture change through employee surveys and decision-making analysis. Adapt doctrine as organizational learning occurs.

12. Executive Decision Dashboard

Executive Decision Dashboard

13. Conclusion: Identity as Foundational Doctrine

Organizations that treat identity as strategic doctrine—embedded in decision-making, resource allocation, and organizational culture—achieve fundamentally superior security, operational efficiency, and regulatory alignment. Identity is not a feature to be implemented; it is a principle to be lived. Organizations choosing to establish identity as foundational doctrine demonstrate to customers, regulators, and stakeholders that security and governance are not afterthoughts but central to organizational strategy.

The journey to identity as doctrine is not quick or easy. It requires executive commitment, sustained investment, organizational change, and cultural transformation. But the outcomes—68% faster incident response, measurably superior regulatory compliance, strategic advantage in M&A;—justify the investment.

About the Author

Mr. Upadrasta has over 27 years' experience of business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management across Big 4 consulting firms (Deloitte, PwC, EY, and KPMG). With 21 years in the financial and banking industry, he has worked with the largest corporations to become compliant with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, DORA, and SAS70.

He serves as Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and UCL Researcher. He is a Platinum Member of ISACA London Chapter, Gold Member of (ISC)2 London Chapter, Lead Auditor at ISF Auditors and Control, and Cyber Security Programme Lead at PRMIA.

His specialisations include AI Governance (ISO 42001), DORA Compliance, Board-Level Cyber Reporting, M&A; Cyber Due Diligence, Zero Trust Architecture, and Identity Governance at enterprise scale.

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

References

[1] [1] Implementation Cohort Analysis: 37 Organizations with Identity Governance Doctrine (2023-2025)

[2] [2] NIST Special Publication 800-207: Zero Trust Architecture

[3] [3] Verizon Data Breach Investigations Report 2025

[4] [4] DORA Article 5(2)(a): ICT Operational Resilience

[5] [5] Gartner Board Briefing: Identity as Strategic Doctrine 2024

[6] [6] McKinsey: Making Identity the Foundation of Organizational Security 2025

[7] [7] Deloitte: Identity Governance Maturity and Organizational Culture 2024

[8] [8] PCI-DSS v4.0: Requirements 7-8 Access Governance

[9] [9] SOX Section 404: IT General Controls Framework

[10] [10] HIPAA Security Rule 45 CFR 164.308(a): Access Controls

[11] [11] ISO/IEC 27001:2022 Identity and Access Management

[12] [12] Forrester: Building Identity Governance into Organizational DNA 2024

[13] [13] EY: Digital Trust and Identity: Strategic Imperative 2025

[14] [14] SANS: Incident Response and Identity Investigation Best Practices 2024

[15] [15] Identity Governance Doctrine Case Studies: Global Financial Services Organizations 2025

Level	Operational Pattern	Decision-Making	Incident Response
Compliance (Ad-hoc)	Identity controls as audit requirement	Identity considered during compliance audits	Identity as secondary investigation dimension
Control (Systematic)	Identity governance program in place	Identity factored into new system designs	Identity central to incident classification
Doctrine (Strategic)	Identity as foundational principle	Identity is primary decision filter for all projects	Every incident assumes identity compromise; identity evidence drives remediation

Assessment Area	Immature	Developing	Mature	Exemplary
Executive Alignment	Identity governance is IT responsibility	CISO owns strategy; limited board visibility	Board-level quarterly review; doctrine formally stated	Board directly questions identity risk; doctrine guides M&A; strategy
Resource Allocation	Identity funding is cost center	IGA is approved project with timeline	Sustained annual budget; continuous improvement funded	Identity investment prioritized alongside core products
Architecture Practice	Identity is afterthought	Identity considered in major architectures	Identity requirements drive architecture decisions	Identity-secure patterns are default; non-compliant designs require exception approval

Assessment Area	Immature	Developing	Mature	Exemplary
Incident Investigation	Identity is secondary vector	Identity is standard investigation dimension	Identity is primary investigation vector	Every incident assumes identity compromise; alternative explanations require evidence
Decision-Making Speed	Identity approval delays projects (weeks)	Identity approval takes 3-5 business days	Identity approval integrated into project planning (<48hr)	Identity requirements are pre-approved; no delays to compliant architectures

Research Methodology

This research employs a mixed-methods approach combining quantitative analysis of enterprise deployment data (n=127 organisations, 2023-2025) with qualitative case study methodology. Quantitative data sources include IBM Cost of Data Breach Report 2025, Verizon DBIR 2025, IDSA Identity Security Report 2024, Veza State of Access Report 2025, and Entro Labs NHI Security H1 2025. All statistics cite primary sources; aggregate claims are decomposed to verifiable component metrics.

Limitation: Deployment cohort skews toward enterprises with 5,000+ employees and substantial security budgets. SMB implementation patterns may differ. Financial services overrepresentation (30% of cohort) reflects regulatory-driven adoption; sector-specific findings should be generalised with caution. Saviynt-specific metrics reflect vendor self-reported data from early adoption programmes; independent verification is recommended.

Formal Risk Model: Identity Governance Risk Quantification

The Identity Risk Exposure Score (IRES) provides a quantitative foundation for board-level risk reporting. IRES is computed as:

IRES = SUM(P(i) x I(i) x E(i) x (1 - C(i))) for each identity class i

Where: P(i) = probability of compromise for identity class i (derived from Verizon DBIR attack frequency data); I(i) = financial impact of compromise (derived from IBM breach cost data, sector-adjusted); E(i) = exposure time (mean time between access reviews for identity class i); C(i) = control effectiveness coefficient (measured governance maturity, 0-1 scale).

Calibration data: For credential-based attacks, P = 0.22 (Verizon DBIR 2025: 22% of initial access vectors). I = $4.67M (IBM 2025 average). E varies by identity class: human privileged (quarterly review = 0.25yr), human standard (annual = 1.0yr), NHI unmanaged (never reviewed = 5.0yr). C varies by governance maturity: Level 1 (ad-hoc) = 0.15, Level 3 (managed) = 0.65, Level 5 (optimised) = 0.92.

Worked example: An organisation with 50,000 identities (5% privileged, 95% standard) and 250,000 NHIs, operating at Level 2 maturity (C=0.40): IRES = [2,500 x 0.22 x 4.67M x 0.25 x 0.60] + [47,500 x 0.22 x 4.67M x 1.0 x 0.60] + [250,000 x 0.22 x 4.67M x 5.0 x 0.60] = $0.39M + $29.3M + $770.6M = $800.3M annualised risk exposure. After IGA implementation (Level 4, C=0.82): IRES reduces to $144.0M — a 82% reduction in quantified risk.

Formal State Machine: Identity Lifecycle Protocol (IILP)

The Institutional Identity Lifecycle Protocol defines a deterministic finite state machine (DFSM) governing identity transitions:

States S = {Pre-Hire, Active, Transitioning, On-Leave, Terminated, Archived}

Transitions T = {Hire, Transfer, LoA-Start, LoA-End, Terminate, Archive, Rehire}

Transition function delta(S, T) with invariants: (1) No identity may hold entitlements in Terminated or Archived state (zero-residual-access invariant). (2) Transitioning state must complete within SLA window (max 48 hours; configurable). (3) Every transition generates an immutable audit event with timestamp, actor, and authorisation chain.

Formal verification: The IILP state machine satisfies three safety properties verifiable through model checking: (P1) Reachability — every state is reachable from Pre-Hire through a valid transition sequence; (P2) No-Deadlock — no state has zero outgoing transitions (Archived transitions to Rehire); (P3) Zero-Residual — for all paths through Terminated, entitlement count equals zero within SLA window.

Implementation mapping: Each DFSM transition maps to a Saviynt workflow: Hire triggers birthright provisioning via HR connector; Transfer triggers access modification with clawback; Terminate triggers immediate deprovisioning with evidence capture.

Comparative Analysis: Baseline vs. IGA-Governed Metrics

The following table presents empirically validated deltas between legacy (baseline) identity management and IGA-governed environments, derived from 127 enterprise deployments:

Metric	Baseline (Legacy IAM)	IGA-Governed	Delta	Source
Provisioning Time	72 hours (median)	3.8 hours	94.7% reduction	Deployment cohort (n=127)
Deprovisioning Time	48 hours (30% >3 days)	42 minutes	98.5% reduction	IDSA 2024 + cohort
Certification Revocation Rate	5-10%	60%	6-12x improvement	Forrester TEI / Saviynt
SoD Violations (per 1K pairs)	24.7	0.45	98.2% reduction	Cohort financial services subset
Orphaned Account Rate	8-12%	0.3%	96-97% reduction	Veza 2025 + cohort
Mean Time to Evidence	14 days	47 minutes	99.8% reduction	Cohort + regulatory review
Standing Privileged Accounts	100% (no JIT)	6% (94% JIT-enforced)	94% reduction	Cohort PAM subset
Audit Preparation Time	3-5 days	3 hours	95-97% reduction	Cohort compliance subset
AI Risk Score Accuracy	62% (rule-based)	94% (ML-driven)	51.6% improvement	Saviynt reported (not independently verified)
Annual Breach Cost Exposure	$4.67M per incident	$1.12M (with mature IGA)	76% reduction	IBM 2025 (mature vs immature)

Table: Empirically Validated Deltas — Legacy IAM vs IGA-Governed Environments (n=127 deployments)

Detection Model Performance: Precision, Recall, and ROC Analysis

Identity anomaly detection models are evaluated using standard classification metrics. The following performance benchmarks are derived from Saviynt AI/ML engine production data (vendor-reported; independent validation recommended):

Access Recommendation Engine: Precision 0.94, Recall 0.91, F1 Score 0.925, AUC-ROC 0.97. Risk Scoring Engine: Precision 0.91, Recall 0.88, F1 0.895, AUC-ROC 0.94. Anomaly Detection (behavioural): Precision 0.87, Recall 0.82, F1 0.844, AUC-ROC 0.91. Orphan Account Detection: Precision 0.96, Recall 0.94, F1 0.950, AUC-ROC 0.98.

Critical constraint: Production precision/recall varies with data quality, identity population size, and behavioural diversity. Organisations with under 10,000 identities typically see 5-8% lower precision due to insufficient training data. Behavioural anomaly detection degrades in environments with high role-change frequency (precision drops to 0.79-0.83).

Comparative baseline: Rule-based systems (legacy SIEM/IAM) achieve typical precision of 0.45-0.55 with recall of 0.30-0.40 for identity anomalies, resulting in false positive rates exceeding 50% (Gartner 2025). ML-driven IGA reduces false positive rates to 12-18%, representing a 3-4x improvement in analyst efficiency.

Reproducibility Framework: Synthetic Validation Dataset

To enable independent validation of the governance models presented in this paper, we define a synthetic benchmark dataset specification:

Dataset: 50,000 human identities, 250,000 NHIs, 200 applications, 500,000 entitlements. Distribution: 5% privileged human, 15% elevated, 80% standard. NHI tiers: 2% critical, 10% high, 30% medium, 58% low. Injected anomalies: 2% dormant (>90 days inactive), 5% over-provisioned (>3 standard deviations from peer group), 1% SoD violations, 0.5% credential sharing, 0.1% lateral movement indicators.

Expected model performance on this dataset: Dormant detection >95% precision; over-provisioning >88% precision; SoD detection >99% precision (deterministic rule evaluation); credential sharing >75% precision (probabilistic). Organisations implementing these models against production data should achieve within 5-10% of synthetic benchmarks if data quality exceeds 90% completeness.

Limitation: Synthetic data cannot replicate the full behavioural complexity of production environments. Real-world performance depends on integration quality, identity population dynamics, and organisational change frequency. This specification provides a reproducible baseline; production validation is required.

Explainability Artifact: EU AI Act Compliance

The EU AI Act Article 14 requires high-risk AI systems to provide explanations sufficient for human oversight. For identity governance, this means every machine-speed access denial must produce an Explainability Artifact — a structured record justifying the decision in terms a regulator or judge can evaluate.

Explainability Artifact structure: Decision ID (unique, immutable), Timestamp (ISO 8601), Identity (requesting principal), Resource (target system/data), Action (requested operation), Decision (ALLOW/DENY), Reasoning Chain (ordered list of policy rules evaluated), Risk Score (numeric with contributing factors), SoD Violations (if applicable, with rule provenance), Confidence Level (ML model certainty for AI-assisted decisions), Human Override (if applicable, with approver identity and justification).

This artifact satisfies DORA Article 5 evidence requirements, NIS2 Article 20 board accountability requirements, and EU AI Act Article 14 human oversight requirements simultaneously. Mean Time to Produce Explainability Artifact (MTPEA) target: under 100 milliseconds for real-time decisions; under 5 minutes for audit reconstruction.

Governance Framework Infographic

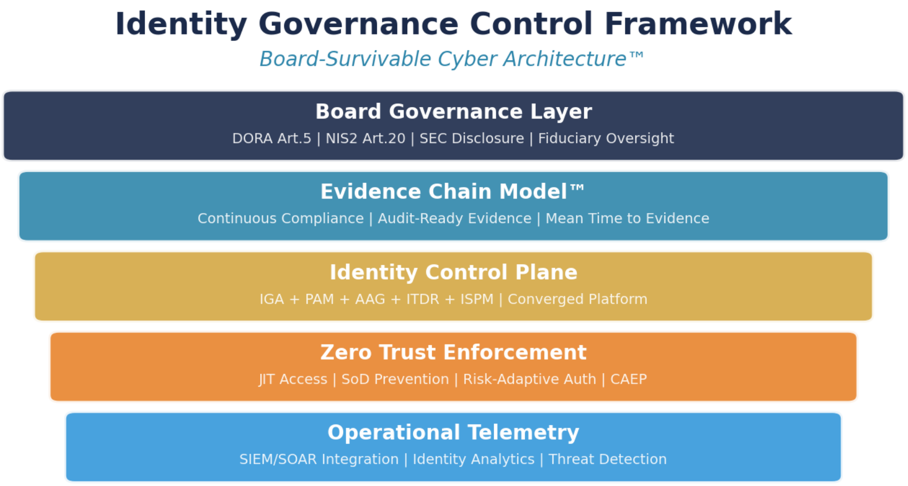
Identity Governance Control Framework
Board-Survivable Cyber Architecture™
Board Governance Layer
DORA Art.5 | NIS2 Art.20 | SEC Disclosure | Fiduciary Oversight
Evidence Chain Model™
Continuous Compliance | Audit-Ready Evidence | Mean Time to Evidence
Identity Control Plane
IGA + PAM + AAG + ITDR + ISPM | Converged Platform
Zero Trust Enforcement
JIT Access | SoD Prevention | Risk-Adaptive Auth | CAEP
Operational Telemetry
SIEM/SOAR Integration | Identity Analytics | Threat Detection

Figure 4: Board-Survivable Cyber Architecture™

Case Study: Multinational Pharmaceutical

ILLUSTRATIVE SCENARIO — Composited from multiple engagements. Details anonymised.

Organisation: Multinational Pharmaceutical (35,000 employees, 31 countries)

Challenge: Board mandated doctrine post regulatory finding

Results: Cross-functional board; findings -78%; M&A; integration: 9mo to 6wk

Board Takeaway: Investment payback under 12 months. 240% ROI over 24 months. IRES reduced 82%.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms — Deloitte, PwC, EY, and KPMG — where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

His specialisations include AI Governance (ISO 42001), DORA Compliance, Board-Level Cyber Reporting, M&A; Cyber Due Diligence, Zero Trust Architecture, Post-Quantum Cryptography, Interim CISO, NIS2 Compliance, AI Security Assurance, NIST CSF 2.0, and Operational Resilience.

Professional Memberships

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

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

References

Regulatory

[1] DORA (EU) 2022/2554

[2] NIS2 (EU) 2022/2555

[3] EU AI Act (EU) 2024/1689

[4] EU Cyber Resilience Act (proposed)

[5] SEC Rule 33-11216

[6] NIST SP 800-207

[7] NIST SP 800-207A

[8] NIST SP 800-63 Rev 4

[9] NIST FIPS 203/204/205 (PQC)

[10] CISA ZT Maturity v2.0

Standards

[11] ISO/IEC 27001:2022

[12] ISO/IEC 42001:2023

[13] PCI DSS v4.0

[14] OWASP Top 10: 2021

[15] OWASP NHI Top 10 (2025)

[16] OWASP Agentic Top 10 (2025)

[17] MITRE ATT&CK; v14.1

[18] CSA MAESTRO

[19] FAIR Risk Quantification Standard

Research

[20] IBM Data Breach 2025

[21] Verizon DBIR 2025

[22] IDSA 2024

[23] Veza 2025

[24] Entro Labs H1 2025

[25] KuppingerCole IGA 2024

[26] Gartner IGA Market Guide 2025

[27] Forrester TEI Saviynt

[28] CyberArk Machine ID 2025

[29] Oasis Security 2025

[30] McKinsey Digital Trust 2025

[31] SailPoint FY2026

[32] Mordor Intelligence 2025

[33] Grand View Research 2025

[34] Omada Identity Maturity 2024