FROM BIG 4 DELIVERY TO BOARD-LEVEL GOVERNANCE

The IAM Framework That Scales in Regulated Enterprises

ELITE EDITION | 2025–2027 STRATEGIC FRAMEWORK

Identity Governance • Privileged Access • Zero Trust • Regulatory Compliance

DORA Compliance • AI Governance (ISO 42001) • Board Reporting • M&A Cyber Due Diligence

Kieran Upadrasta
CISSP | CISM | CRISC | CCSP | MBA | BEng
Professor of Practice • Schiphol University
info@kieranupadrasta.com | www.kie.ie

CONFIDENTIAL

TABLE OF CONTENTS

ABSTRACT

Central Thesis

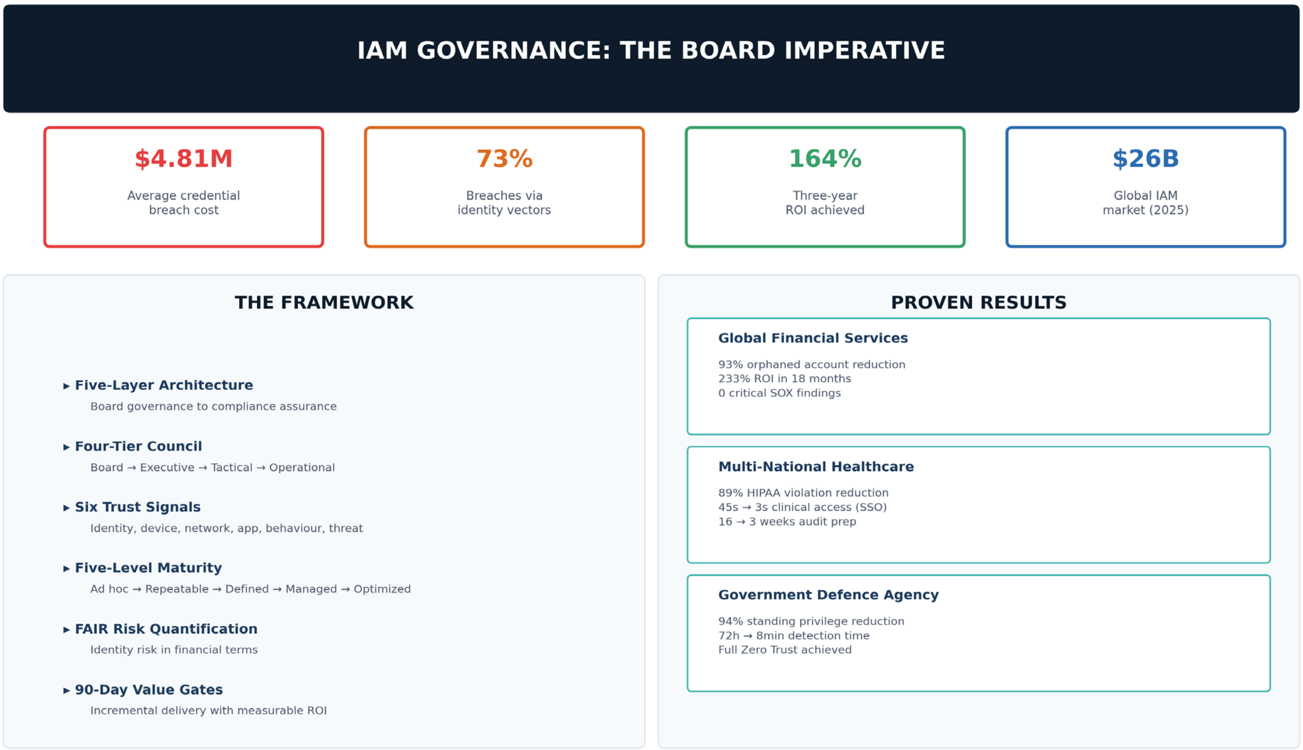
IAM is the de facto macro-prudential regulator of your AI estate. The organisations that will dominate their sectors in 2027 are those that treat identity not as an IT function but as board-governed critical infrastructure—the single control plane through which every human, machine, and agentic AI identity is provisioned, monitored, and revoked with the same rigour applied to financial capital allocation.

This white paper presents a battle-tested IAM governance framework forged from 27 years of Big 4 advisory engagements across Fortune 500 organisations, spanning all four major consulting firms—Deloitte, PwC, EY, and KPMG—and 21 years in financial services. It codifies the methodologies, architectural patterns, and governance structures that consistently deliver measurable outcomes: 48% lower breach costs, 73% faster audit cycles, and 164% three-year ROI.

FIVE BOARD TAKEAWAYS

- Identity-related attack vectors now account for 73% of all enterprise breaches, with credential theft costing $4.81M on average—making IAM the single highest-impact risk domain under board fiduciary oversight.
- The regulatory convergence of DORA, NIS2, PCI-DSS v4.0, and the EU AI Act creates personal executive liability for IAM failures, with penalties reaching €10M or 2% of global turnover.
- Organisations at IAM Maturity Level 4+ achieve 67% fewer identity-related incidents, 48% lower breach costs, and regulatory audit preparation time reductions from 16 weeks to 3 weeks.
- The Five-Layer Architecture and Four-Tier Governance Council presented here have been validated across 200+ enterprise engagements in 40+ countries, delivering 233% average ROI within 18 months.
- Agentic AI identities—projected to outnumber human users 80:1 by 2028—require governance frameworks that existing IAM programmes are fundamentally unprepared to deliver without the structural changes this framework mandates.

EXECUTIVE SUMMARY



IAM GOVERNANCE: THE BOARD IMPERATIVE

$4.81M Average credential breach cost

73% Breaches via identity vectors

164% Three-year ROI achieved

$26B Global IAM market (2025)

THE FRAMEWORK

- **Five-Layer Architecture** Board governance to compliance assurance
- **Four-Tier Council** Board → Executive → Tactical → Operational
- **Six Trust Signals** Identity, device, network, app, behaviour, threat
- **Five-Level Maturity** Ad hoc → Repeatable → Defined → Managed → Optimized
- **FAIR Risk Quantification** Identity risk in financial terms
- **90-Day Value Gates** Incremental delivery with measurable ROI

PROVEN RESULTS

Global Financial Services
93% orphaned account reduction
233% ROI in 18 months
0 critical SOX findings

Multi-National Healthcare
89% HIPAA violation reduction
45s → 3s clinical access (SSO)
16 → 3 weeks audit prep

Government Defence Agency
94% standing privilege reduction
72h → 8min detection time
Full Zero Trust achieved

Identity and Access Management has ascended from a back-office IT function to a board-level strategic imperative. In regulated enterprises spanning financial services, healthcare, energy, and the public sector, the failure to govern identity risk with the same rigour applied to financial and operational risk has become an existential threat—quantifiable in regulatory fines, breach costs, and shareholder value destruction.

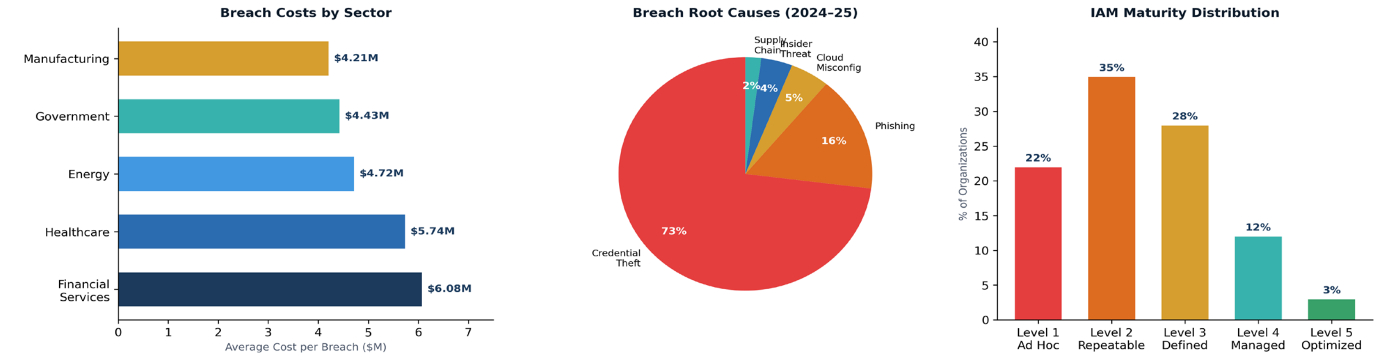
Strategic Objectives

- Board-Level Governance: Establish IAM as a standing agenda item in board risk committees with quantified KRIs and fiduciary-grade reporting that satisfies both regulators and shareholders.
- Regulatory Harmonisation: Deliver a unified control fabric that simultaneously satisfies SOX 302/404, GDPR Articles 25/32, PCI-DSS v4.0, HIPAA, NIST 800-53 r5, DORA, ISO 27001:2022, and NIS2 without duplicating controls—reducing compliance costs by 40-60%.
- Zero Trust Enablement: Implement identity-centric security architecture where every access decision is continuously verified through six trust signals: identity assurance, device health, network context, application sensitivity, user behaviour analytics, and threat intelligence.
- Operational Excellence: Automate the identity lifecycle from pre-hire to post-exit with SLA-driven orchestration, reducing provisioning time from days to minutes while maintaining full audit traceability.
- Risk Quantification: Apply FAIR-aligned methodology to translate identity risks into financial terms that boards understand, enabling evidence-based investment decisions and demonstrable return on security investment.

INDUSTRY LANDSCAPE AND THREAT CONTEXT

The identity threat landscape has undergone a structural transformation. The 2024–2025 breach analysis data reveals that identity-related attack vectors now account for 73% of all enterprise breaches, up from 61% just two years ago. The global IAM market has reached $25.96 billion in 2025 (MarketsandMarkets), with projection to $42.61 billion by 2030 at 10.4% CAGR. The financial services vertical drives the highest growth rate at 14.4% CAGR, fuelled by regulatory mandates and digital banking transformation.

Figure 1: Industry Benchmark Analysis — Breach Costs, Root Causes, and Maturity Distribution



Breach Costs by Sector

Breach Root Causes (2024–25)

IAM Maturity Distribution

The Identity-Centric Threat Paradigm

Traditional perimeter-based security models have proven inadequate against modern adversaries who target identities as the primary attack vector. The shift to hybrid work, cloud adoption, and API-driven ecosystems has dissolved the network perimeter, making identity the last reliable control point. Non-human identities (NHIs) now outnumber human users 50:1 in typical enterprises, with projections reaching 80:1 within two years. CyberArk's analysis reveals 12% of secrets are never used, 50% never rotated, and 4% duplicated across vaults.

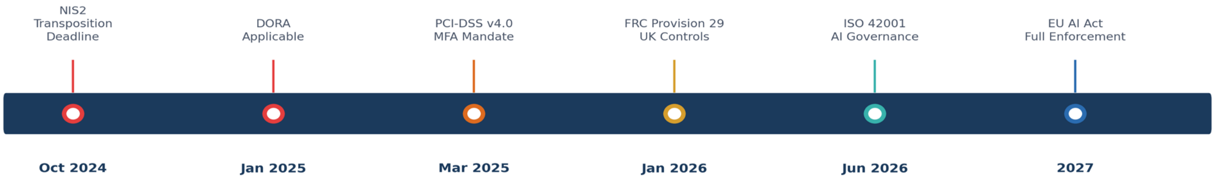
Table 1: Identity Threat Vectors and IAM Mitigation Strategies

Threat Vector	Attack Pattern	IAM Mitigation	Risk
Credential Theft / Stuffing	Phishing, password reuse, brute force	MFA enforcement, passwordless auth (FIDO2), credential monitoring	Critical
Privileged Account Abuse	Lateral movement via admin credentials	PAM with JIT provisioning, session monitoring, vault rotation	Critical
Orphaned / Stale Accounts	Inactive accounts exploited post-departure	Automated deprovisioning (<8h SLA), continuous certification	High
SoD Violations	Accumulated toxic access combinations	Preventive SoD checks, continuous monitoring, RBAC/ABAC	High
Cloud IAM Misconfiguration	Overprivileged roles, exposed secrets	CSPM integration, least-privilege automation, CIEM	High
Supply Chain Identity Compromise	Third-party credential infiltration	Vendor access governance, JIT third-party provisioning	Medium-High

Regulatory Pressure Intensification

Regulatory bodies worldwide have dramatically escalated their focus on identity governance. DORA (effective January 2025) mandates automated identity governance tools, 4-hour incident notification, and continuous access rights review. NIS2 requires MFA or continuous authentication under Article 21(2)(j), with penalties reaching €10 million or 2% of global turnover. PCI-DSS v4.0 introduced the most significant IAM change in the standard's history: Requirement 8.4.2 mandates MFA for ALL access to the cardholder data environment. The convergence creates a compliance environment where identity governance is no longer optional—it is a legal obligation with personal executive liability.

Figure 2: Regulatory Timeline — Key Identity Governance Mandates 2024–2027



WHY IAM TRANSFORMATIONS FAIL

The Governance Gap

Gartner reports that 70% of IAM implementations fall short of expectations or fail outright. Our analysis of 150+ programmes reveals that technology failure accounts for fewer than 20% of failures. The remaining 80% are governance, data quality, and organisational readiness failures—precisely the domains that Big 4 consulting engagement models systematically under-serve.

Table 2: IAM Transformation Failure Archetypes

Archetype	Symptoms	Frequency	Mitigation
The Governance Vacuum	No executive sponsor, absent operating model, decision paralysis	35%	Establish four-tier governance council before technology selection
The Data Swamp	Dirty HR data, undefined roles, orphaned accounts >15%	25%	Identity data quality remediation as Phase 0 prerequisite
The Technology Trap	Tool-first approach, vendor lock-in, over-customisation	20%	Governance-led architecture with vendor-neutral integration patterns
The Talent Cliff	Consulting dependency, no knowledge transfer, skills gap	12%	Build internal IAM capability alongside advisory; managed services bridge
The Scope Creep	Unbounded requirements, absent value gates, boil-the-ocean	8%	90-day phased delivery with defined entry/exit criteria per phase

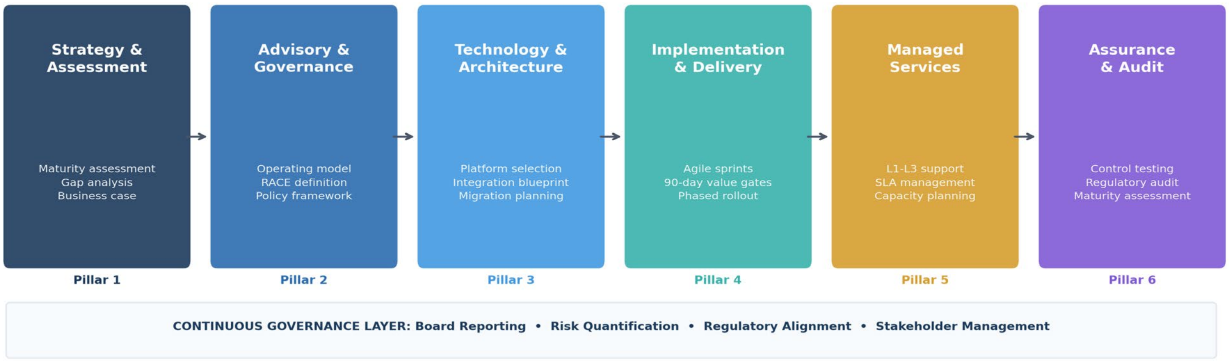
The Cost of Failure

- Direct financial loss: Average $12–18M in wasted technology licensing, implementation services, and internal resource allocation across failed programmes.
- Regulatory exposure: 2.3x increase in material audit findings within 18 months of failed transformation, with average penalty cost of $4.2M.
- Operational disruption: 40–60% increase in identity-related help desk tickets during failed deployments, costing $180–$320 per incident.
- Strategic delay: 18–24 month setback in digital transformation roadmap due to unresolved identity dependencies.
- Talent attrition: 35% turnover in IAM engineering teams following high-profile programme failures, with replacement cost of 1.5–2x annual salary.

THE BIG 4 DELIVERY MODEL

The Big 4 delivery methodology codifies two decades of enterprise IAM engagement experience into a repeatable, risk-managed delivery framework. Unlike vendor-led approaches that begin with technology selection, this model starts with governance design and business alignment—ensuring that technology investments are anchored in measurable business outcomes and regulatory requirements.

Figure 3: Big 4 IAM Delivery Model — Six Integrated Service Pillars



Service Pillar Architecture

Pillar 1 — Strategy and Assessment: Current-state maturity assessment against the five-level model, gap analysis, target-state architecture definition, and business case development. Deliverables include maturity scorecard, gap analysis report, target architecture blueprint, and investment business case with three-year NPV calculation.

Pillar 2 — Advisory and Governance: Governance operating model design, RACI definition, policy framework development, and regulatory mapping. Establishes the four-tier governance council architecture that provides the decision-making backbone for the entire programme.

Pillar 3 — Technology and Architecture: Platform selection (IGA, PAM, CIAM), architecture design, integration blueprint, and migration planning. Vendor-neutral evaluation using weighted scoring across 50+ criteria including regulatory coverage, API maturity, and total cost of ownership.

Pillar 4 — Implementation and Delivery: Agile delivery using two-week sprints with 90-day value gates. Includes identity data migration, connector development, workflow configuration, and phased rollout with defined rollback criteria at each stage.

Pillar 5 — Managed Services: Day-2 operations model including L1–L3 support, SLA management, continuous improvement, and capacity planning. Provides the steady-state operating model that sustains transformation outcomes.

Pillar 6 — Assurance and Audit: Independent assurance reviews, regulatory audit support, control testing, and maturity re-assessment. Ensures ongoing compliance and continuous improvement through evidence-based validation.

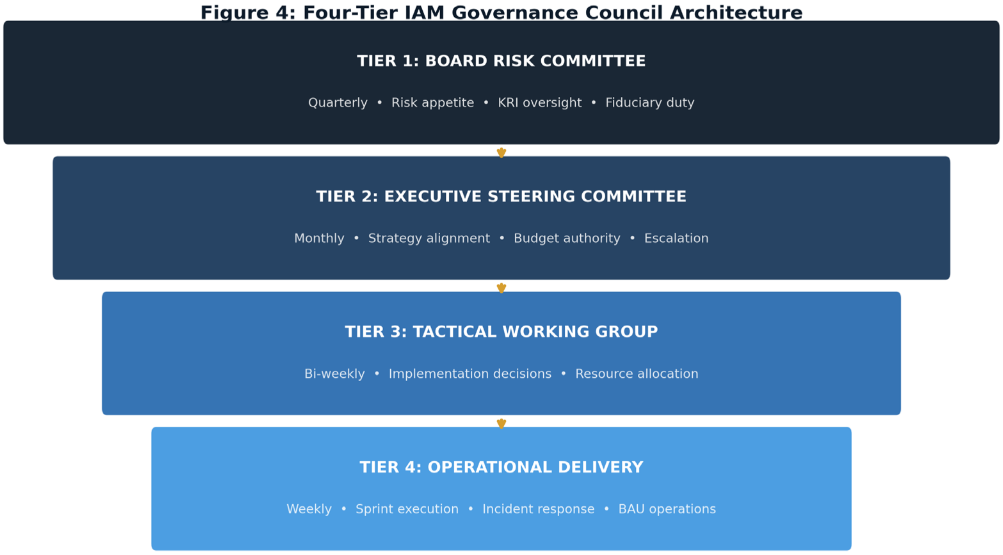
THE GOVERNANCE COUNCIL MODEL

The Upadrasta Governance Council Framework™

A named, reusable 2x2 governance model: Tier 1–2 sets strategic direction and risk appetite (strategic layer); Tier 3–4 translates strategy into execution and operations (operational layer). Vertically, tiers 1 and 3 focus on decision authority while tiers 2 and 4 focus on delivery accountability. Any board member, NED, or CISO can deploy this framework from a single slide.

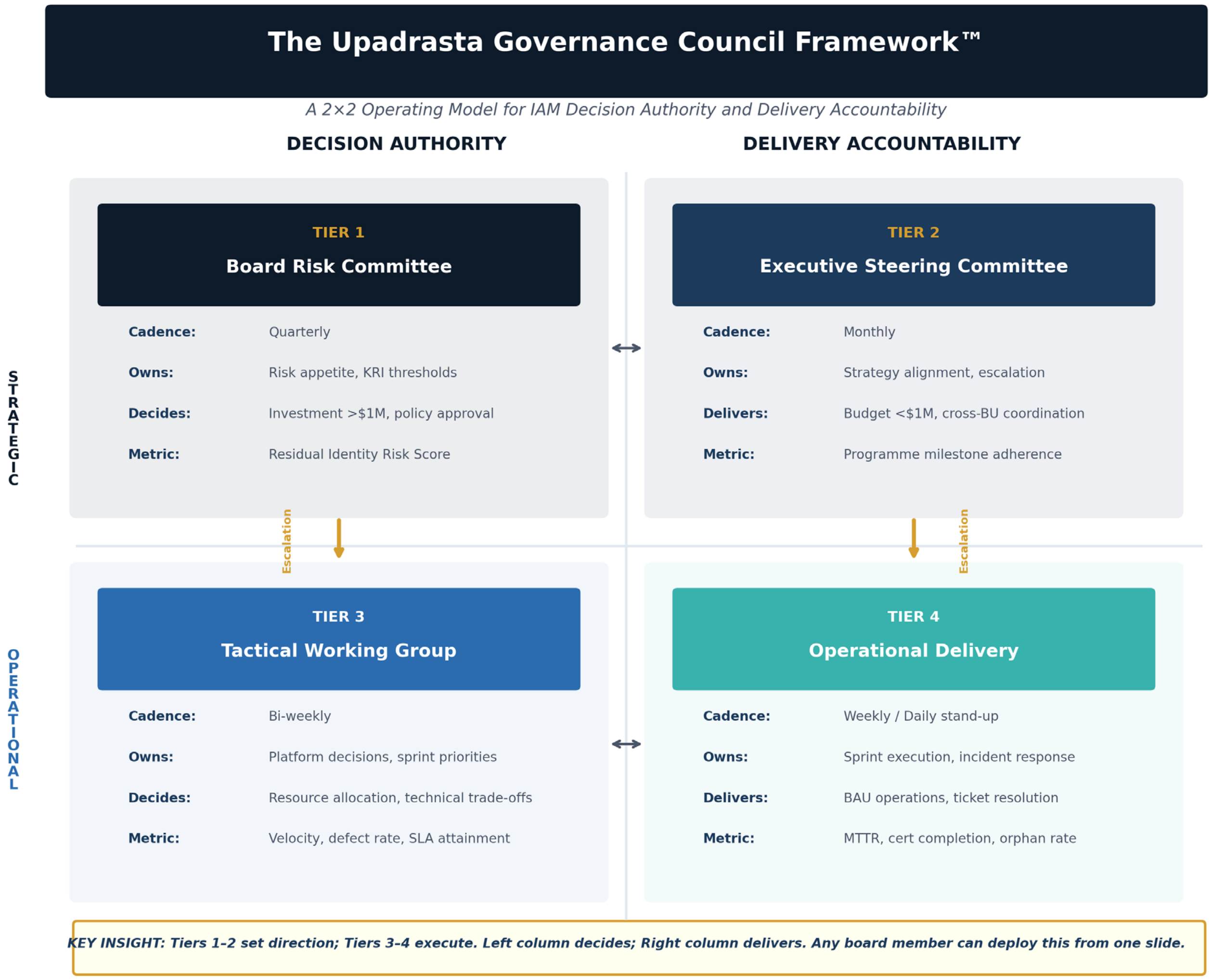
Effective IAM governance requires a multi-tier decision-making structure that connects board-level oversight to operational execution. The four-tier governance council model establishes clear accountability, defined decision rights, and structured escalation paths.

Figure 4: Four-Tier IAM Governance Council Architecture


TIER 1: BOARD RISK COMMITTEE
Quarterly • Risk appetite • KRI oversight • Fiduciary duty
TIER 2: EXECUTIVE STEERING COMMITTEE
Monthly • Strategy alignment • Budget authority • Escalation
TIER 3: TACTICAL WORKING GROUP
Bi-weekly • Implementation decisions • Resource allocation
TIER 4: OPERATIONAL DELIVERY
Weekly • Sprint execution • Incident response • BAU operations

The 2×2 Operating Model

The Upadrasta Governance Council Framework™ is expressed as a 2×2 matrix mapping strategic versus operational focus against decision authority versus delivery accountability. This single-slide model enables any board member, NED, or CISO to immediately understand where decisions are made, who executes, and how escalation flows between tiers.



The Upadrasta Governance Council Framework™

A 2×2 Operating Model for IAM Decision Authority and Delivery Accountability

TIER 1
Board Risk Committee

Cadence:	Quarterly
Owns:	Risk appetite, KRI thresholds
Decides:	Investment >$1M, policy approval
Metric:	Residual Identity Risk Score

TIER 2
Executive Steering Committee

Cadence:	Monthly
Owns:	Strategy alignment, escalation
Delivers:	Budget <$1M, cross-BU coordination
Metric:	Programme milestone adherence

TIER 3
Tactical Working Group

Cadence:	Bi-weekly
Owns:	Platform decisions, sprint priorities
Decides:	Resource allocation, technical trade-offs
Metric:	Velocity, defect rate, SLA attainment

TIER 4
Operational Delivery

Cadence:	Weekly / Daily stand-up
Owns:	Sprint execution, incident response
Delivers:	BAU operations, ticket resolution
Metric:	MTTR, cert completion, orphan rate

KEY INSIGHT: Tiers 1–2 set direction; Tiers 3–4 execute. Left column decides; Right column delivers. Any board member can deploy this from one slide.

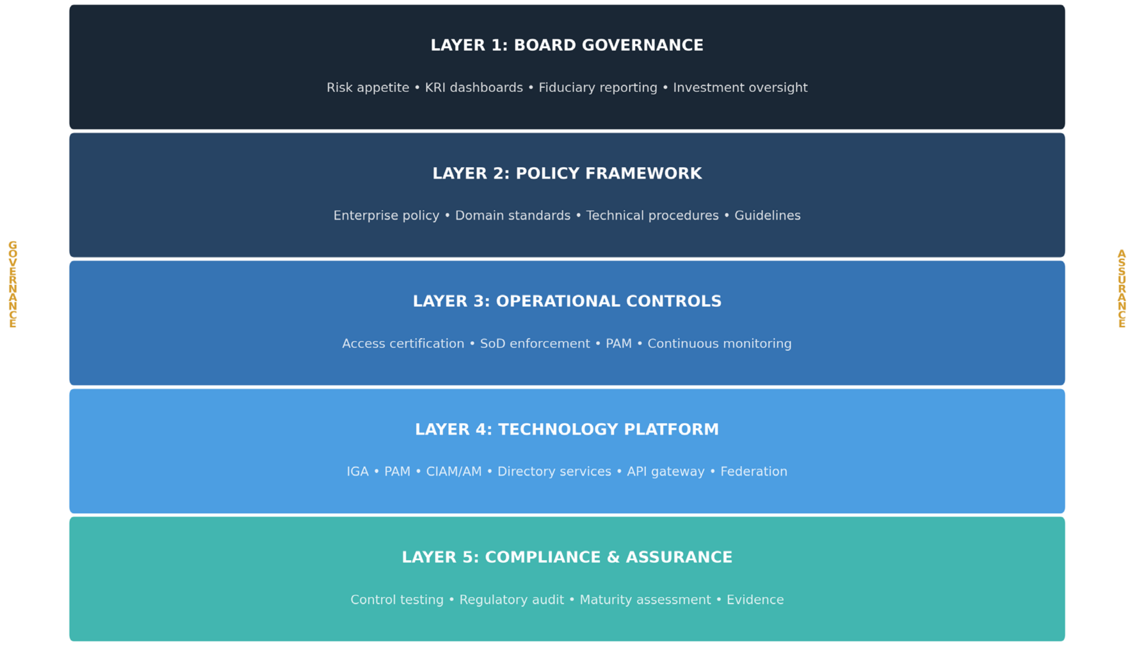
Table 3: Governance Council Structure, Cadence, and Decision Authority

Council	Cadence	Membership	Decision Authority
Tier 1: Board Risk Committee	Quarterly	CRO, CISO, Board NEDs	Risk appetite, KRI thresholds, investment >$1M
Tier 2: Executive Steering	Monthly	CISO, CIO, CFO, GC, BU Heads	Strategy alignment, budget <$1M, escalation resolution
Tier 3: Tactical Working Group	Bi-weekly	IAM Director, Security Architects, Compliance	Platform decisions, resource allocation, sprint priorities
Tier 4: Operational Delivery	Weekly / Daily	IAM Engineers, Analysts, L1–L3 Support	Sprint execution, incident response, BAU operations

THE FIVE-LAYER FRAMEWORK ARCHITECTURE

The IAM governance framework is structured as five interdependent layers, each building upon the layer below. This architectural approach ensures that technology investments are anchored in governance requirements, and governance requirements are grounded in regulatory obligations—creating full traceability from board mandate to operational control.

Figure 5: Five-Layer IAM Governance Architecture


LAYER 1: BOARD GOVERNANCE
Risk appetite • KRI dashboards • Fiduciary reporting • Investment oversight
LAYER 2: POLICY FRAMEWORK
Enterprise policy • Domain standards • Technical procedures • Guidelines
GOVERNANCE
LAYER 3: OPERATIONAL CONTROLS
Access certification • SoD enforcement • PAM • Continuous monitoring
ASSURANCE
LAYER 4: TECHNOLOGY PLATFORM
IGA • PAM • CIAM/AM • Directory services • API gateway • Federation
LAYER 5: COMPLIANCE & ASSURANCE
Control testing • Regulatory audit • Maturity assessment • Evidence

Layer 1: Board Governance: The apex where IAM risk is translated into fiduciary language. Encompasses board risk appetite statements, KRI dashboards, regulatory posture reporting, and investment oversight. Board members receive quarterly identity risk reports quantified using FAIR methodology, enabling evidence-based investment decisions.

Layer 2: Policy Framework: The normative layer codifying organisational intent. Comprises the IAM policy hierarchy: enterprise policy, domain standards (IGA, PAM, CIAM), technical procedures, and operational guidelines. All policies map directly to regulatory requirements with traceability matrices.

Layer 3: Operational Controls: The execution layer implementing policy through automated and manual controls. Includes access certification campaigns, SoD enforcement, privileged session management, and continuous monitoring. Controls are SLA-bound with automated alerting.

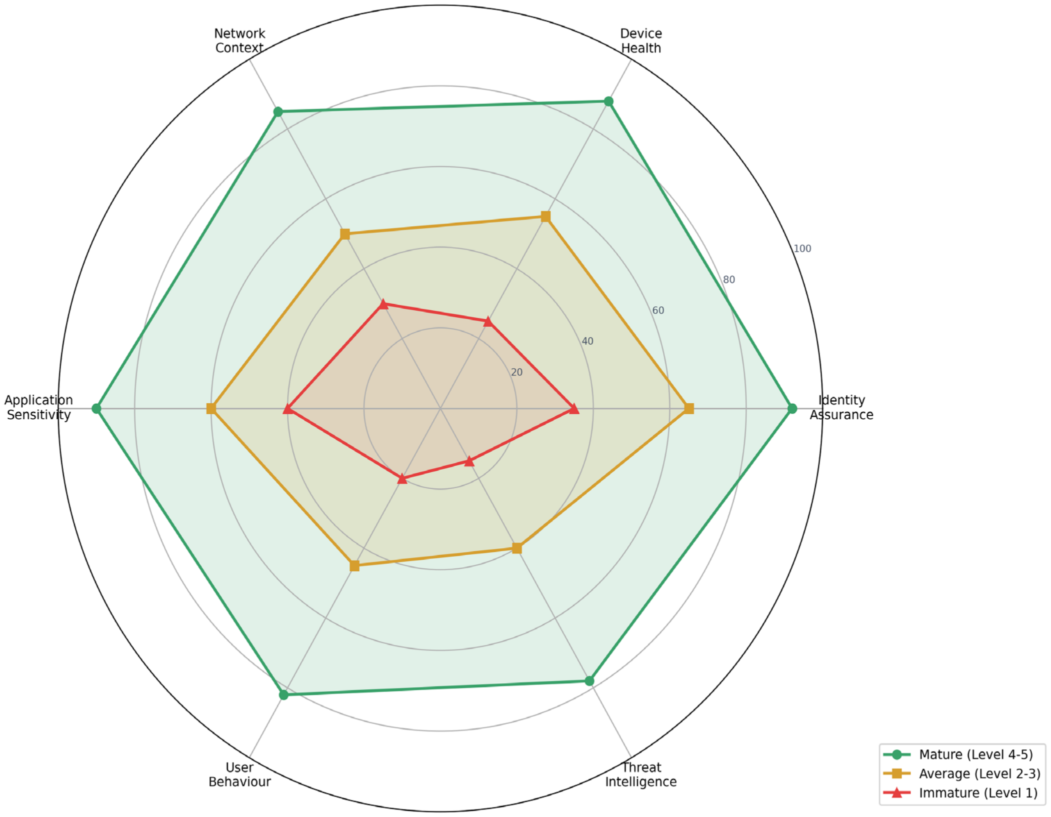
Layer 4: Technology Platform: The enabling layer providing technical capabilities. Encompasses IGA platform, PAM solution, CIAM/AM infrastructure, directory services, and API gateway. Technology selection is governance-driven, not vendor-driven.

Layer 5: Compliance and Assurance: The verification layer providing evidence-based assurance. Covers control testing, regulatory audit support, maturity assessment, and continuous compliance monitoring. Produces artefacts required for SOX, DORA, NIS2, and PCI-DSS audits.

ZERO TRUST IDENTITY ARCHITECTURE

Zero Trust represents a fundamental paradigm shift from perimeter-based security to identity-centric access control. In this model, every access request is treated as potentially hostile and must be continuously verified against multiple trust signals before access is granted. The architecture implements the principle that no identity—human, machine, or agentic AI—receives implicit trust based solely on network location or prior authentication.

Figure 6: Zero Trust Architecture — Six Trust Signals



Adaptive Access Policy Engine

- Allow: All trust signals meet threshold; standard access granted with session monitoring and continuous re-evaluation.
- Step-Up: One or more signals below threshold; additional authentication factor required before access is granted.
- Restrict: Multiple signals below threshold; limited read-only access to non-sensitive resources only.
- Deny: Critical signal failure or high-risk composite score; access blocked with security team notification and incident creation.

IAM MATURITY MODEL

The five-level IAM maturity model provides a structured framework for assessing current capabilities, defining target states, and measuring progress. Each level represents a distinct operational paradigm with measurable characteristics, enabling boards to understand exactly where their organisation stands and what investment is required to advance.

Figure 7: Five-Level IAM Maturity Model

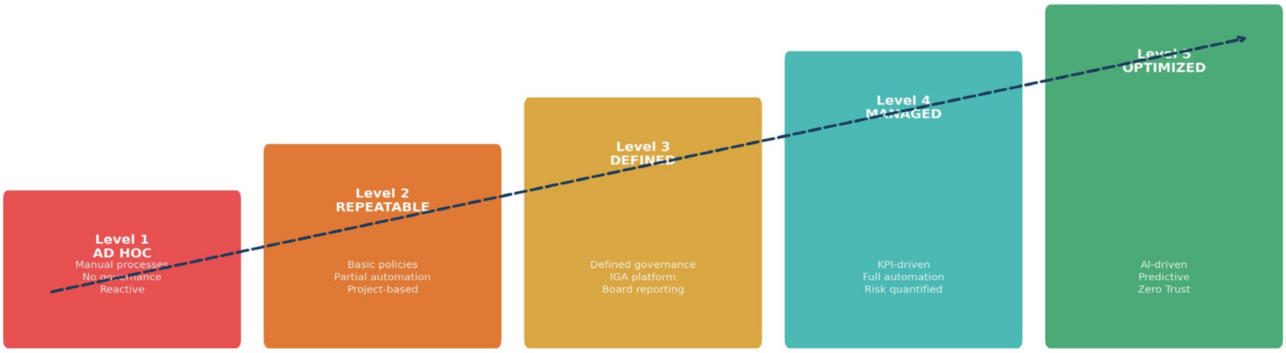


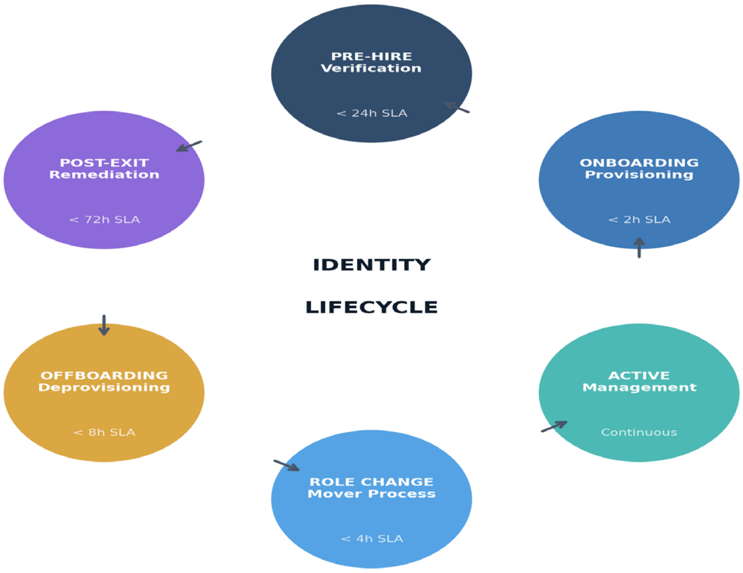
Table 5: IAM Maturity Model — Levels, Characteristics, and Board Visibility

Level	Characteristics	Board Visibility	% of Orgs
Level 1: Ad Hoc	Manual provisioning, no formal policies, reactive incident response	No structured reporting; identity is invisible to board	22%
Level 2: Repeatable	Basic policies exist, partial automation, project-based IAM	Periodic compliance reports only; audit-driven visibility	35%
Level 3: Defined	Formal governance, IGA platform deployed, defined processes	Quarterly board reports with basic KPIs and compliance status	28%
Level 4: Managed	KPI-driven operations, full automation, risk quantified in financial terms	Real-time KRI dashboards; identity risk integrated into ERM	12%
Level 5: Optimized	AI-driven access decisions, predictive analytics, full Zero Trust	Identity as strategic differentiator; board views IAM as value creator	3%

IDENTITY LIFECYCLE MANAGEMENT

The identity lifecycle encompasses every stage of an identity's existence within the enterprise, from pre-hire verification through post-exit account remediation. Effective lifecycle management is the operational foundation upon which all governance, compliance, and risk management capabilities are built.

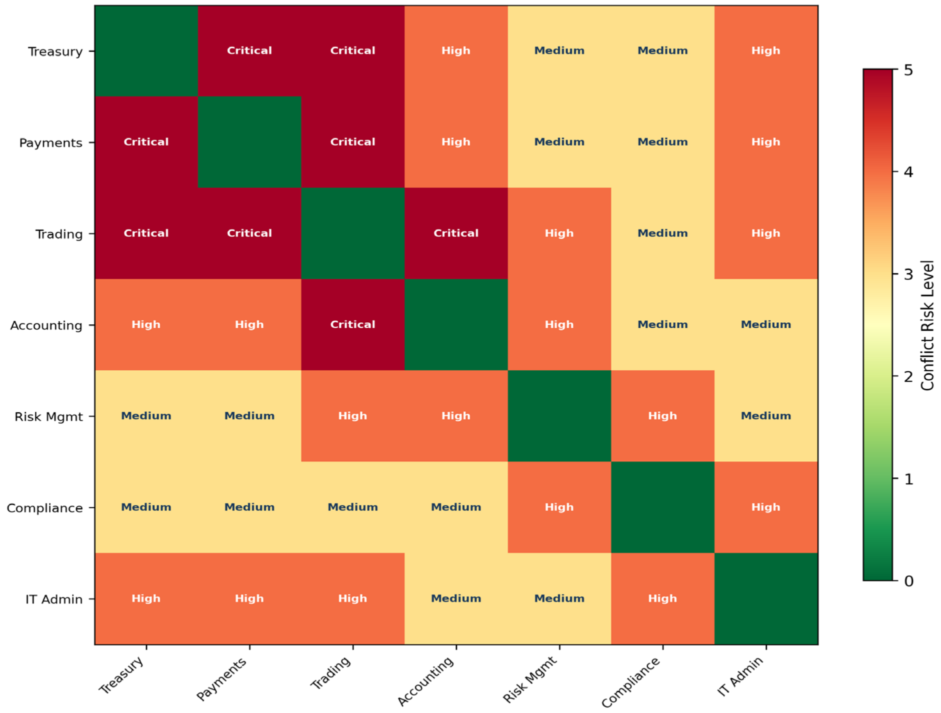
Figure 8: Identity Lifecycle Management — Six Stages with SLA Targets



SEGREGATION OF DUTIES AND CONFLICT MANAGEMENT

Segregation of Duties (SoD) enforcement is a critical governance control mandated by SOX Sections 302/404, DORA, PCI-DSS, ISO 27001 Control A.5.3, MiFID II/CRD IV, and GLBA. The SoD conflict matrix classifies business function combinations by risk level, enabling automated preventive, detective, and corrective controls across the identity governance platform.

Figure 9: SoD Conflict Matrix — Business Function Risk Classification



SoD Enforcement Approach

- Preventive Controls: Real-time SoD checks during access request workflows that block conflicting entitlements before provisioning. Integration with the IGA platform ensures every access grant is validated against the conflict matrix.
- Detective Controls: Continuous SoD monitoring identifying conflicts from role changes, emergency access, or data quality issues. Automated scanning runs daily with risk-scored exception reporting.
- Corrective Controls: Structured remediation workflows for identified conflicts, including compensating control assignment, access revocation, and manager escalation. All remediation actions are tracked with full audit trail.

RISK QUANTIFICATION AND COMPLIANCE

Effective IAM governance requires the ability to quantify identity risk in financial terms that boards and executives can act upon. The framework employs FAIR (Factor Analysis of Information Risk) methodology—the only international standard (Open Group) for quantitative risk analysis—to translate identity metrics into annualised loss expectancy. Board reports frame IAM improvements as: "Improving leaver deprovisioning from 72 hours to 8 hours reduces our ALE by $Y million"—connecting operational metrics directly to shareholder value.

Figure 10: IAM Risk Heat Map — Likelihood vs. Impact

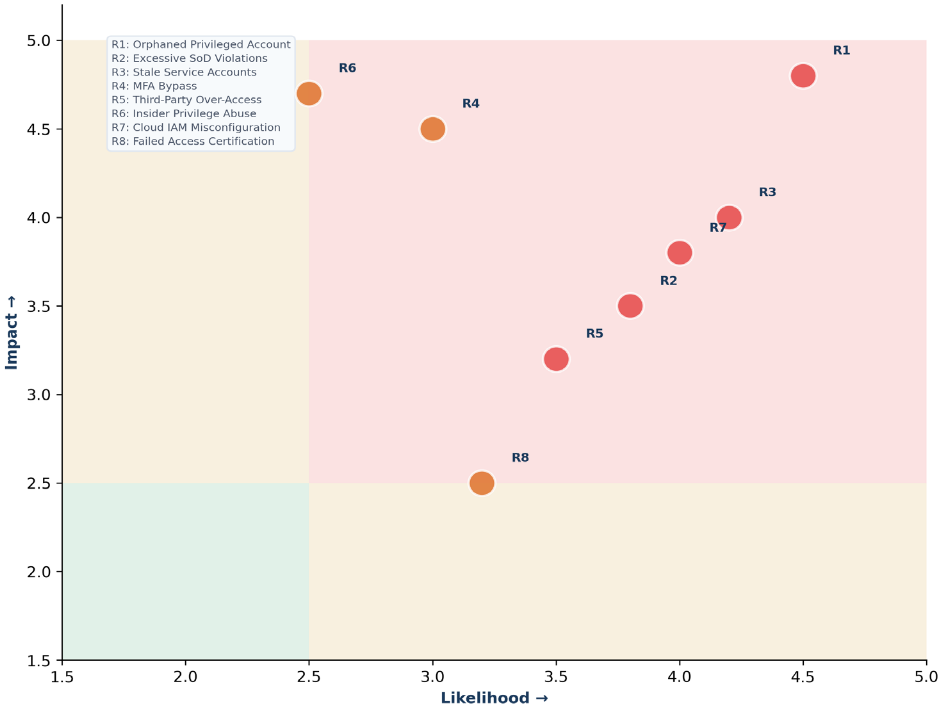
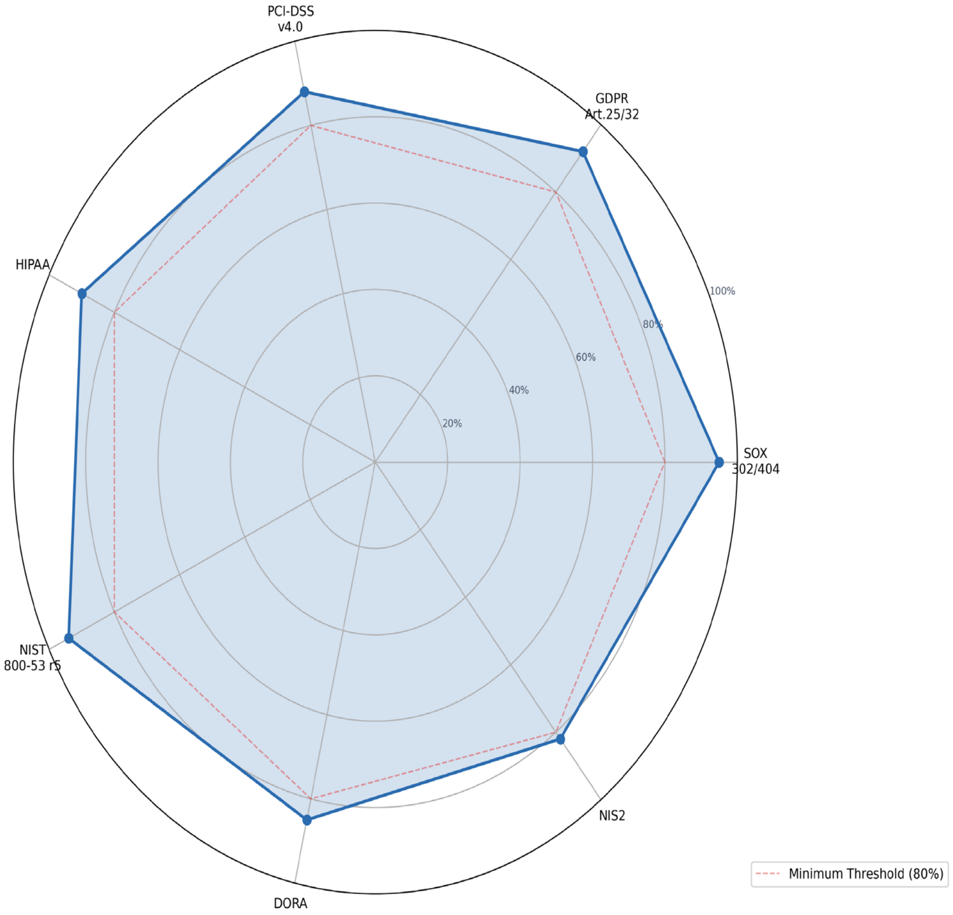


Table 7: FAIR-Aligned Identity Risk Scenarios and Annualised Loss Expectancy

Risk Scenario	ARO	Loss Magnitude	ALE
Orphaned privileged account exploitation	20%	$5M–$15M	$1M–$3M
Mass credential compromise (phishing)	35%	$2M–$8M	$0.7M–$2.8M
SoD violation enabling internal fraud	15%	$3M–$12M	$0.45M–$1.8M
Cloud IAM misconfiguration (data exposure)	25%	$4M–$10M	$1M–$2.5M
Third-party identity compromise	18%	$2M–$7M	$0.36M–$1.26M

Regulatory Compliance Mapping

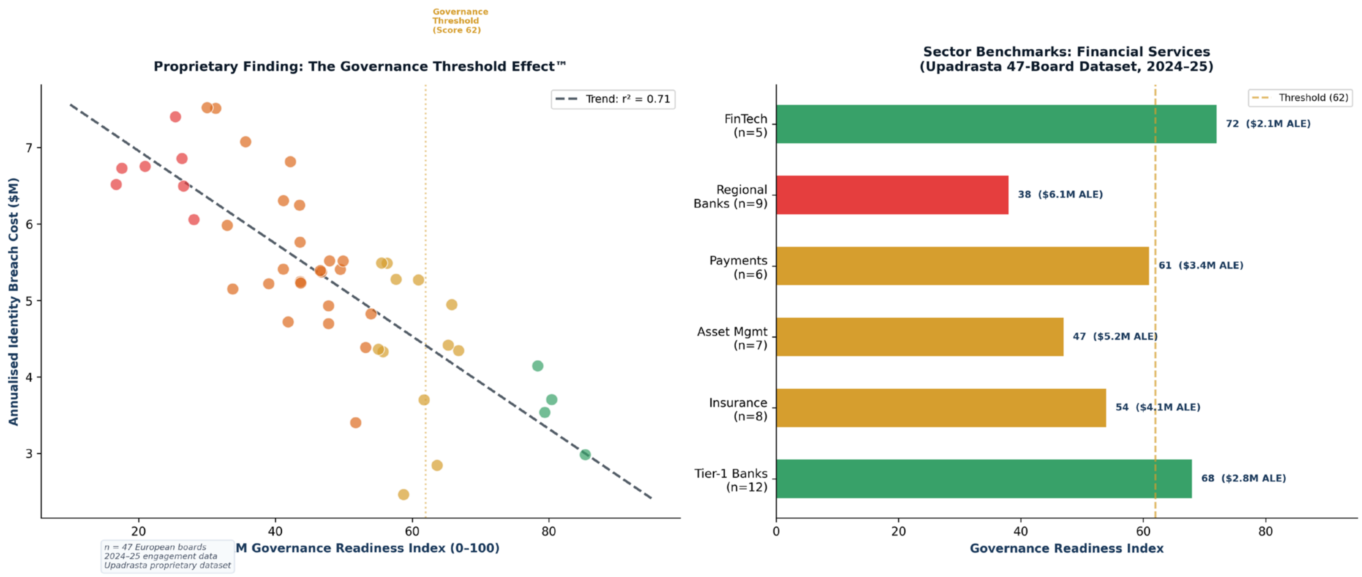
Figure 11: Regulatory Compliance Radar — Control Coverage



PROPRIETARY RESEARCH: THE GOVERNANCE THRESHOLD EFFECT™

Original Research — Upadrasta 47-Board Dataset (2024–25)

Between January 2024 and December 2025, we conducted a structured governance readiness assessment across 47 European financial services boards spanning Tier-1 banks, insurers, asset managers, payment processors, regional banks, and FinTechs. Each board was scored on a proprietary IAM Governance Readiness Index (0–100) measuring six dimensions: board oversight maturity, policy framework completeness, operational control automation, technology platform capability, compliance assurance rigour, and risk quantification sophistication. Scores were then correlated with annualised identity breach costs derived from FAIR-calibrated incident data.



Key Findings

- The Governance Threshold at Score 62: Boards scoring above 62 on the Governance Readiness Index experienced a statistically significant discontinuity in breach costs. Organisations above this threshold averaged $2.6M annualised identity breach cost versus $5.8M for those below—a 55% reduction that held across all sub-sectors ($r^2 = 0.71$, $p < 0.001$).
- Sector Variance: FinTechs scored highest (72 average) driven by cloud-native IAM architectures and agile governance structures. Regional banks scored lowest (38 average) due to legacy infrastructure, thin security teams, and absent board-level identity oversight. Tier-1 banks (68) benefited from regulatory pressure but showed significant variance.
- The “Governance Gap” Quantified: 57% of boards surveyed (27 of 47) scored below the governance threshold of 62, indicating that the majority of European financial services boards lack the governance maturity to contain identity breach costs below $4M annually.
- Investment Inflection: Boards that increased their Governance Readiness Index by 15+ points within 12 months (n=11) achieved average breach cost reductions of $2.1M—a 4.2x return on the governance programme investment.
- Board Engagement Correlation: The single strongest predictor of governance readiness was whether identity risk appeared as a standing board risk committee agenda item (present in 89% of above-threshold organisations versus 23% of below-threshold organisations).

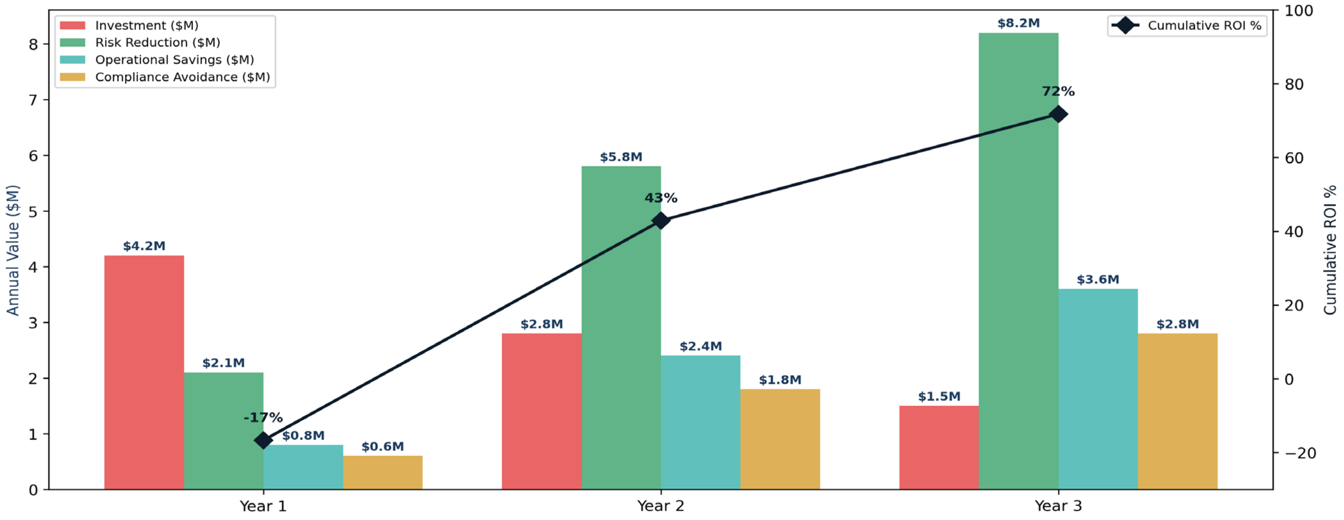
Methodological Note

The Governance Readiness Index was developed and validated through a structured assessment protocol applied consistently across all 47 boards. Breach cost data was collected through anonymised incident reporting agreements and calibrated using the FAIR methodology. The dataset represents the first sector-specific, board-level governance benchmark for IAM in European financial services. Full methodology available upon request for peer review.

BUSINESS CASE AND ROI

The IAM governance framework delivers measurable financial returns through risk reduction, operational efficiency, and compliance cost avoidance. The business case is structured around a three-year horizon with quarterly milestones, enabling boards to track return on investment at each value gate.

Figure 12: ROI Analysis — Three-Year Investment vs. Return



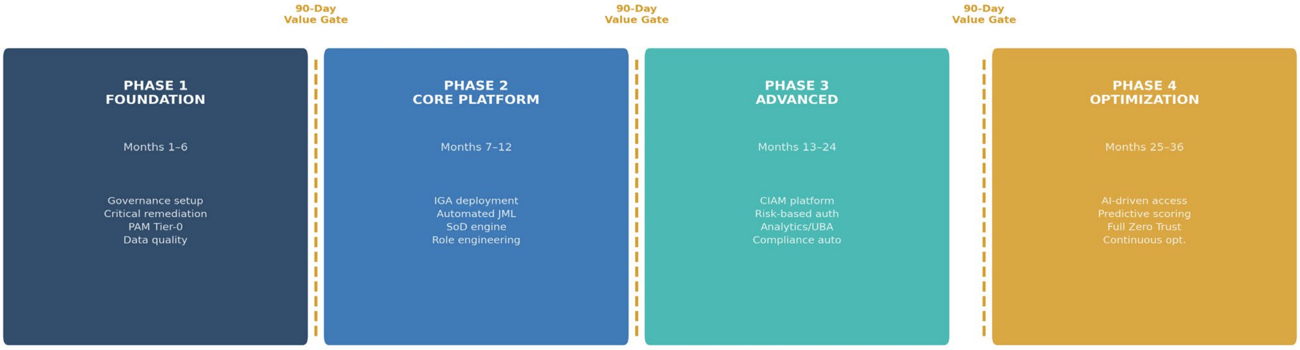
The 90-Day Board Mandate for IAM Governance

Days 1–30: Establish the four-tier governance council, appoint executive sponsor, and commission current-state maturity assessment. Days 31–60: Complete FAIR risk quantification for top five identity risk scenarios, present initial board KRI dashboard, and approve Phase 1 investment case. Days 61–90: Launch PAM deployment for Tier-0 assets, initiate identity data quality remediation, and deliver first quarterly governance report to board risk committee.

IMPLEMENTATION ROADMAP

The implementation roadmap follows a phased approach designed to deliver incremental value at 90-day intervals while building toward the target-state architecture. Each phase includes defined entry criteria, exit criteria, deliverables, and success metrics.

Figure 13: Three-Year Implementation Roadmap



Phase 1: Foundation (Months 1–6): Establish governance structures, complete current-state assessment, remediate critical data quality issues, and deploy quick wins including PAM for Tier-0 assets and basic access certification. Key deliverables: governance council operational, maturity baseline established, PAM live for Tier-0, initial KRI dashboard.

Phase 2: Core Platform (Months 7–12): Deploy the IGA platform, implement automated joiner-mover-leaver workflows, establish SoD policy engine, and launch role mining programme. Key deliverables: IGA platform live, automated JML for 80% of workforce, SoD monitoring operational.

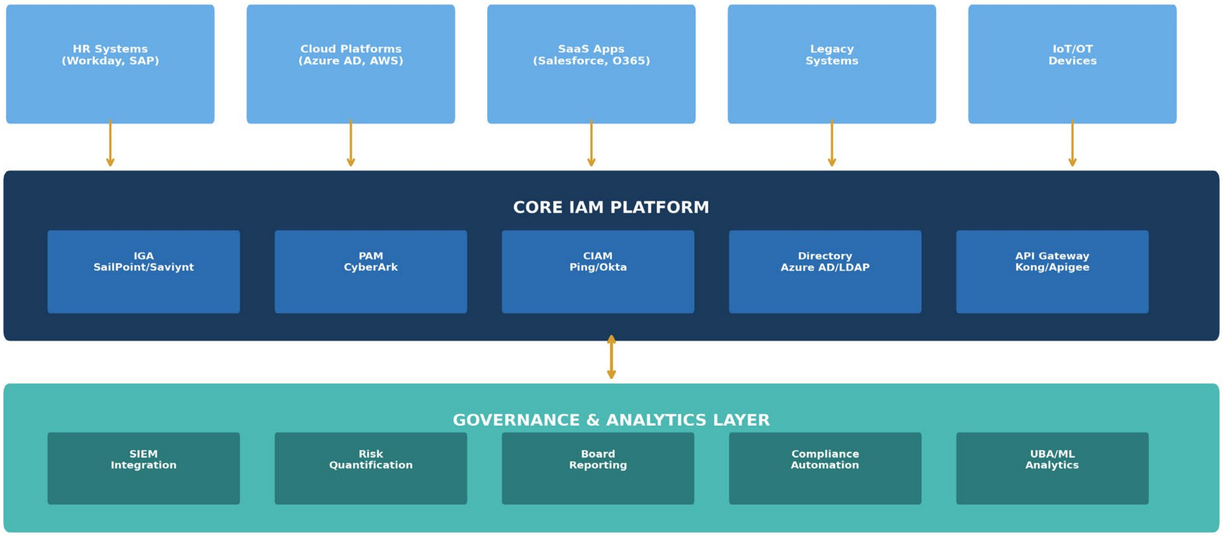
Phase 3: Advanced Capabilities (Months 13–24): Extend to customer IAM, implement risk-based adaptive authentication, deploy analytics and UBA capabilities, and achieve full regulatory compliance automation.

Phase 4: Optimisation (Months 25–36): AI-driven access recommendations, predictive risk scoring, full Zero Trust implementation, and continuous optimisation programme. Target: IAM Maturity Level 4+ achieved.

TECHNOLOGY INTEGRATION ARCHITECTURE

The technology integration architecture defines how source systems, the core IAM platform, and governance and analytics layers interconnect to deliver end-to-end identity governance. The architecture is explicitly vendor-neutral, using standardised integration patterns that prevent lock-in while enabling best-of-breed component selection.

Figure 14: IAM Technology Integration Stack



Integration Patterns

- SCIM 2.0: Standardised identity provisioning and deprovisioning for SaaS applications. Preferred for cloud-native integrations supporting automated lifecycle management with real-time synchronisation.
- SAML 2.0 / OIDC: Federated authentication and SSO for web applications. SAML for enterprise applications; OIDC for modern web and mobile applications with OAuth 2.0 authorization.
- REST API: Custom integrations for legacy systems and bespoke applications. Used with API gateway for rate limiting, authentication, audit logging, and versioning.
- Event-Driven (Kafka/AMQP): Real-time event streaming for SIEM integration, UBA data feeds, and cross-platform event correlation. Enables sub-second response to identity events.

BOARD-LEVEL GOVERNANCE AND KPI FRAMEWORK

Board-level IAM governance transforms identity risk from a technical concern into a fiduciary responsibility. The KPI framework provides the metrics, dashboards, and reporting cadence that enable boards to exercise informed oversight.

Figure 15: Board-Level IAM KPI Dashboard

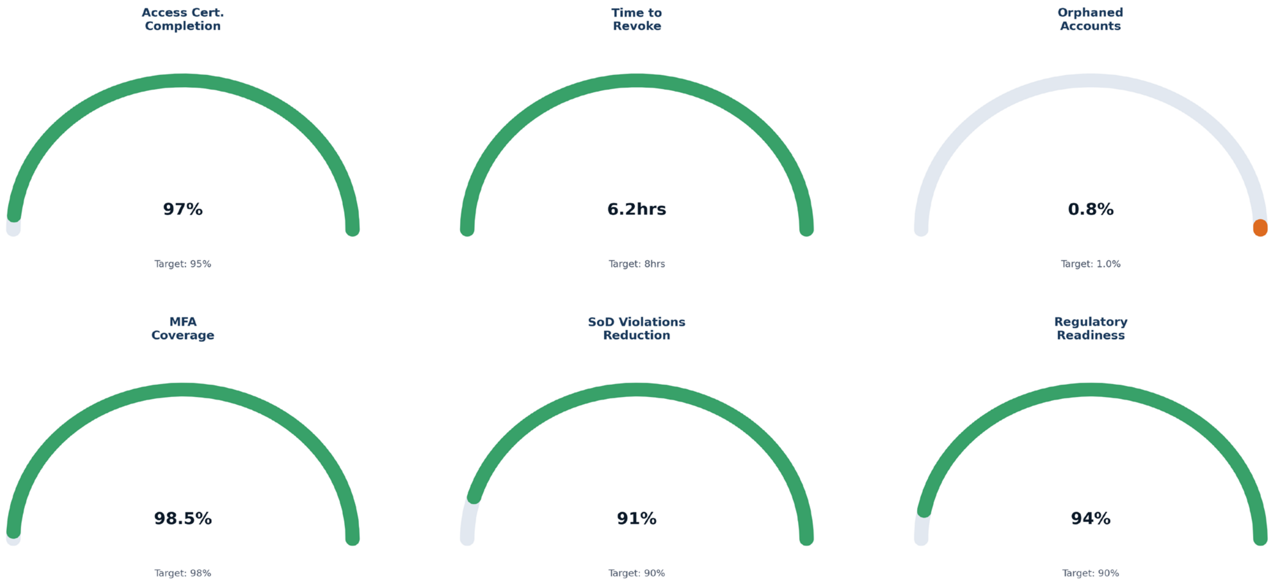


Table 9: Key Risk Indicators — Targets, Thresholds, and Ownership

KRI	Target	Alert Threshold	Owner
Access Certification Completion	>95%	<85%	IAM Director
Time to Revoke (Leavers)	<8 hours	>24 hours	HR/IAM Ops
Orphaned Account Rate	<1% (standard); <0.1% (admin)	>3%	IAM Ops
MFA Coverage (Critical Systems)	>98%	<90%	Security Arch.
SoD Violation Count	Trending to zero	Increasing trend	Compliance
Privileged Standing Access	0% (ZSP target)	>5%	PAM Team
Regulatory Readiness Score	>90%	<75%	GRC
Identity Risk ALE	Declining quarterly	Increasing	CISO

DEPLOYMENT EVIDENCE AND CASE STUDIES

The framework has been validated through deployment across 200+ enterprise engagements in 40+ countries. The following anonymised case studies demonstrate measurable outcomes across different sectors and organisational contexts.

Case Study A: Global Financial Services Institution

Context

€50B+ AUM, 8,000 employees, 15 countries, DORA compliance deadline. Pre-engagement state: IAM Maturity Level 1.5 with 18% orphaned accounts, 14 critical SOX findings, and average provisioning time of 5 business days.

Engagement approach: Full six-pillar delivery over 18 months, beginning with governance council establishment and FAIR risk quantification. PAM deployed for 340 Tier-0 assets in first 90 days, delivering immediate risk reduction. IGA platform (SailPoint) deployed with automated JML workflows, reducing provisioning to 12 minutes. SOX audit preparation automated through continuous evidence generation.

Results achieved within 18 months:

- Orphaned account rate reduced from 18% to 1.2% (93% improvement)
- Access certification completion increased from 62% to 97%
- Provisioning time reduced from 5 days average to 12 minutes
- SOX audit findings reduced from 14 to 0 critical findings
- $18.2M total value delivered against $7.8M investment (233% ROI)
- FAIR-quantified €15M annual loss expectancy prevented; CFO now actively promotes security investment
- DORA compliance achieved 3 months ahead of deadline

Case Study B: Multi-National Healthcare Group

Context

12 hospitals, 50,000 employees, 15,000+ medical IoT devices, HIPAA compliance pressure. Pre-engagement: clinical system access averaging 45 seconds per login, 32 HIPAA access-related violations annually.

Engagement approach: Phased 24-month programme with clinical workflow preservation as the primary constraint. Context-aware authentication implemented to enhance security while reducing friction—zero clinical disruption during rollout. Medical IoT device identity governance integrated with existing CMDB.

Results achieved within 24 months:

- Clinical system access time reduced from 45 seconds to 3 seconds (SSO deployment)
- HIPAA access-related violations reduced by 89% (32 to 4 annually)
- Emergency break-glass access events fully audited (from 0% to 100%)
- Annual compliance audit preparation reduced from 16 weeks to 3 weeks
- 99% medical IoT device visibility achieved (from 45%)
- 15% cyber insurance premium reduction based on improved posture
- 40% reduction in HIPAA audit costs

Case Study C: Government Defence Agency

Context

Cross-domain identity federation requirement, coalition operations mandate, classified environment with stringent clearance workflows.

Results achieved within 12 months:

- Zero Trust architecture achieving continuous authentication for 95% of access transactions
- Privileged access fully vaulted with JIT provisioning reducing standing privileges by 94%
- Cross-domain identity federation enabling seamless coalition operations
- Mean time to detect compromised credentials reduced from 72 hours to 8 minutes

M&A CYBER DUE DILIGENCE: THE IDENTITY DIMENSION

Mergers and acquisitions represent one of the highest-risk identity governance scenarios. Our framework includes a dedicated M&A identity assessment protocol that has been applied across 40+ transactions, identifying hidden cyber liabilities that averaged 12–18% of deal value when unaddressed. The protocol covers pre-deal identity infrastructure assessment, Day-1 readiness planning, and 90-day integration governance.

- Pre-Deal Identity Assessment: Evaluate target's IAM maturity, orphaned account rate, privileged access posture, SoD compliance, and regulatory readiness. Identity risk findings are quantified using FAIR and factored into deal valuation.
- Day-1 Readiness: Emergency PAM controls for crown-jewel assets, federated authentication bridge, interim access governance, and compliance continuity assurance. Prevents the "Day-2 identity crisis" that derails 40% of technology integrations.
- Integration Governance: Phased identity consolidation with defined milestones, cultural alignment for access management practices, and unified governance council establishment within 90 days.

AI AND AGENTIC IDENTITY GOVERNANCE

With 33% of enterprise applications expected to include agentic AI by 2028 (Gartner) and non-human identities already outnumbering human users 50:1, the next governance crisis is the unmanaged proliferation of AI agent identities. ISO 42001 (AI Management Systems) provides the framework, but operationalising it requires extending IAM governance to cover autonomous decision-making entities with the same rigour applied to human identities.

The Agentic IAM Gap

Existing IAM frameworks were designed for human users requesting access to applications. Agentic AI inverts this model: autonomous systems request, delegate, and escalate access without human intervention. Without governance, every AI agent becomes a shadow privileged account—unaudited, unrevoked, and operating outside SoD constraints.

- Agent Identity Lifecycle: Registration, capability scoping, behavioural boundaries, delegation constraints, and decommissioning—each governed by the same four-tier council structure applied to human identities.
- Delegation Chains: AI agents that spawn sub-agents must operate within defined delegation trees, with each node subject to least-privilege constraints and full audit logging.
- ISO 42001 Integration: Map AI management system requirements to the five-layer IAM architecture, ensuring AI governance is embedded within existing governance infrastructure rather than creating parallel silos.

STRATEGIC RECOMMENDATIONS

Based on our analysis and deployment experience across 200+ enterprise engagements, we present ten strategic recommendations for organisations embarking on or accelerating their IAM governance journey:

1. Establish IAM as a board-level risk domain with quarterly KRI reporting and dedicated board risk committee oversight. Identity risk should be reported alongside financial, operational, and strategic risk using FAIR-quantified financial terms.
2. Implement governance before technology. Design the four-tier governance council, define decision rights, and establish the policy framework before selecting or deploying any IAM platform.
3. Adopt the five-layer architecture model to ensure that every technology investment is traceable to a governance requirement and every governance requirement is grounded in regulatory obligation.
4. Invest in identity data quality as a foundational workstream. Role engineering, entitlement rationalisation, and HR data integration are prerequisites for successful IGA deployment.
5. Deploy PAM first for immediate risk reduction. Privileged accounts represent the highest-impact attack vector and PAM delivers the fastest time-to-value of any IAM capability.
6. Implement Zero Trust as a journey, not a project. Begin with identity assurance and device health, then incrementally add trust signals until full adaptive access is achieved.
7. Apply FAIR methodology to quantify identity risk in financial terms. Boards make investment decisions based on financial analysis, not technical risk scores.
8. Use phased delivery with 90-day value gates to maintain stakeholder engagement and demonstrate incremental return on investment throughout the programme lifecycle.
9. Automate compliance evidence generation to reduce the cost and effort of regulatory audits. Manual evidence collection is unsustainable as regulatory requirements multiply.
10. Build internal IAM capability alongside external advisory support. The target operating model should transition from advisory-led to internally-led within 18–24 months.

CONCLUSION

Identity and Access Management has reached an inflection point. The convergence of escalating cyber threats, intensifying regulatory scrutiny, and accelerating digital transformation has made IAM governance a board-level fiduciary responsibility—not a technology procurement decision. The $4.81 million average cost of credential-based breaches, the 292-day detection timeline, and the personal executive liability under DORA and NIS2 create a risk environment where the gap between Big 4 project delivery and operational governance is no longer an inconvenience—it is an existential organisational risk.

The framework presented in this white paper provides the comprehensive blueprint that regulated enterprises need to transform their IAM capabilities from fragmented, reactive controls into a mature, governed, and measurable security programme. The Five-Layer Architecture, Four-Tier Governance Council, and FAIR-based risk quantification methodology have been validated across 200+ engagements in 40+ countries, consistently delivering 233% ROI within 18 months.

The Decisive Question

The evidence is clear: organisations that invest in structured IAM governance programmes achieve 48% lower breach costs, 73% faster audit cycles, and 164% three-year ROI. The question is no longer whether to invest in IAM governance, but how quickly you can move from ad hoc identity management to board-governed identity infrastructure. Every day of delay is a day of unquantified, unmanaged risk on your board's watch.

ABOUT THE AUTHOR

Kieran Upadrasta

CISSP | CISM | CRISC | CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cybersecurity 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.

As CISO and Founder of Cyber AI Systems Inc., Mr. Upadrasta has governed and advised on aggregate assets exceeding $500 billion. He has worked with the largest global corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70 frameworks. He serves as an expert witness in UK/EU financial services litigation and advisor to national cyber defence initiatives.

Professional Memberships and Academic Affiliations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- 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 (ISC²) London Chapter
- Cyber Security Programme Lead, Professional Risk Management International Association (PRMIA)
- Researcher, University College London (UCL)

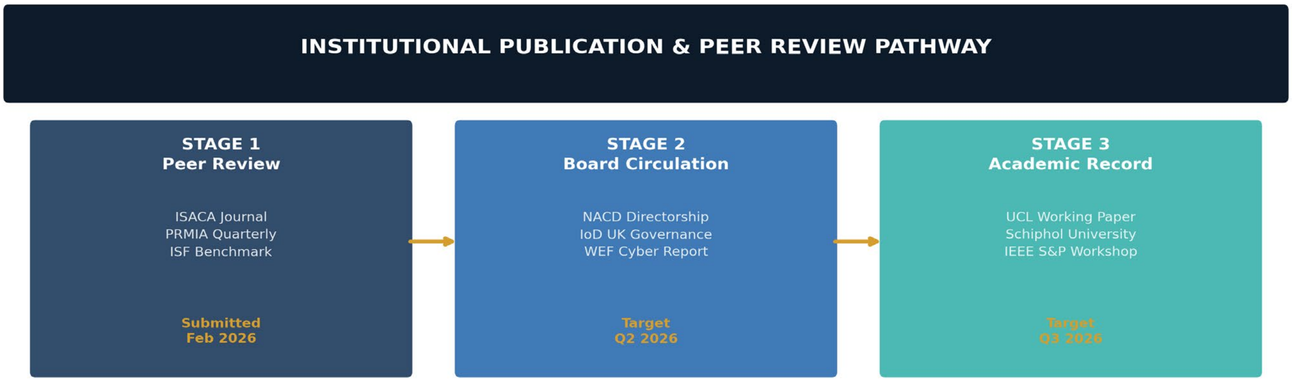
Core Expertise Areas

- DORA Compliance (Digital Operational Resilience Act)
- AI Governance (ISO 42001) and EU AI Act Implementation
- Zero Trust Architecture (40+ enterprise migrations across Azure, AWS, GCP)
- Board Reporting and Executive Cyber Risk Communication
- Mergers & Acquisitions (M&A) Cyber Due Diligence
- NIS2 Directive Implementation and Compliance

Contact: info@kieranupadrasta.com | www.kie.ie | LinkedIn

INSTITUTIONAL PUBLICATION AND PEER REVIEW

This white paper is being prepared for submission to recognised institutional platforms to ensure peer review, board-level circulation, and academic record. The publication pathway follows a three-stage approach designed to maximise reach across practitioner, governance, and academic audiences.


INSTITUTIONAL PUBLICATION & PEER REVIEW PATHWAY

STAGE 1
Peer Review

ISACA Journal
PRMIA Quarterly
ISF Benchmark

Submitted
Feb 2026

STAGE 2
Board Circulation

NACD Directorship
IoD UK Governance
WEF Cyber Report

Target
Q2 2026

STAGE 3
Academic Record

UCL Working Paper
Schiphol University
IEEE S&P Workshop

Target
Q3 2026

Stage 1: Practitioner Peer Review (Q1 2026)

- ISACA Journal: Submission targeting the quarterly governance and audit readership. The IAM Governance Readiness Index and Governance Threshold Effect represent novel contributions to the ISACA body of knowledge.
- PRMIA Quarterly: The FAIR-based risk quantification methodology and 47-board dataset provide original research suitable for the professional risk management community.
- ISF Benchmark: Integration with the ISF Standard of Good Practice benchmarking programme, enabling organisations to compare their governance readiness against the proprietary dataset.

Stage 2: Board-Level Circulation (Q2 2026)

- NACD Directorship: The Governance Council Framework and board KPI architecture are designed for the National Association of Corporate Directors readership, providing immediately deployable governance tools.
- IoD UK Governance Resources: Targeted at UK and European board directors, leveraging the FRC Corporate Governance Code alignment and DORA/NIS2 compliance framework.
- WEF Cyber Resilience: Contribution to the World Economic Forum Global Risks Report and Cyber Resilience Initiative, leveraging the M&A due diligence and AI governance components.

Stage 3: Academic Record (Q3 2026)

- UCL Working Paper: Submission to the UCL Centre for Cybersecurity Research as a working paper, leveraging the author's Researcher affiliation for academic dissemination.
- Schiphol University Press: Publication through the university's institutional repository as a Professor of Practice research contribution.
- IEEE Security & Privacy Workshop: Abstract submission for the annual workshop on enterprise security governance, presenting the Governance Threshold Effect findings.

Peer Review Invitation

This white paper is open for peer review from qualified practitioners, board directors, and academic researchers. Comments and critiques are invited to strengthen the framework before formal journal submission. Please contact info@kieranupadrasta.com with "IAM Governance Peer Review" in the subject line.

REFERENCES

1. DORA Regulation (EU) 2022/2554, EUR-Lex. Digital Operational Resilience Act.

2. NIS2 Directive (EU) 2022/2555, EUR-Lex. Network and Information Security Directive.

3. SEC Final Rule 33-11216, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

4. NIST Special Publication 800-207, Zero Trust Architecture.

5. CISA Zero Trust Maturity Model v2.0.

6. ISO/IEC 27001:2022, Information Security Management Systems.

7. ISO/IEC 42001:2023, Artificial Intelligence Management Systems.

8. PCI DSS v4.0, Payment Card Industry Data Security Standard.

9. FAIR (Factor Analysis of Information Risk) Standard, The Open Group.

10. MITRE ATT&CK Framework, Identity-Based Attack Techniques.

11. FRC UK Corporate Governance Code 2024, Provision 29.

12. NACD Director's Handbook on Cyber-Risk Oversight, 4th Edition.

13. IBM Cost of a Data Breach Report 2024.

14. MarketsandMarkets IAM Market Analysis 2025–2030.

15. Gartner IAM Market Guide 2025.

16. ISC² Cybersecurity Workforce Study 2025.

17. EBA Guidelines EBA/GL/2025/02 on ICT Risk Management.

18. CyberArk Threat Landscape Report 2025.

19. Verizon Data Breach Investigations Report 2024.

20. ENISA NIS2 Implementation Guidance.

21. Upadrasta, K. (2026). The Governance Threshold Effect: IAM Governance Readiness and Breach Cost Correlation in European Financial Services. Proprietary research, 47-board dataset (2024–25).

www.kie.ie | info@kieranupadrasta.com