WHITEPAPER | ELITE EDITION

# Identity Governance as Infrastructure

## Translating Policy into Automated Control Architecture for the Autonomous Enterprise

*Introducing the Autonomous Identity Control Architecture (AICA(TM))*
*Evidence Chain Model(TM) | 12 Regulatory Regimes | 90-Day Deployment*

Doctrine from 40+ Enterprise Transformations | 27 Years Big 4 Experience | 12 Jurisdictions

**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 (Cybersecurity, AI & Quantum Computing), Schiphol University*
*Honorary Senior Lecturer, Imperials | UCL Researcher | ISACA Platinum | (ISC)2 Gold*

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

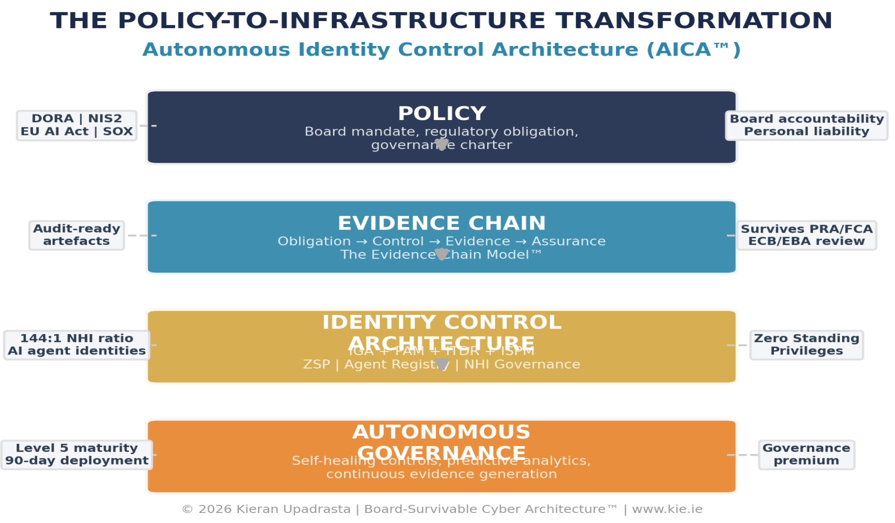
| $26B | 144:1 | 90% | $4.81M |
|---|---|---|---|
| IAM Market | NHI Ratio | Identity Incidents | Breach Cost |

# Table of Contents

**DORA Compliance | AI Governance (ISO 42001) | Board Reporting | M&A Cyber Due Diligence | Zero Trust Architecture**

# 1. Executive Summary: The Identity Crisis

***Identity governance has become the operating system of enterprise security.***


THE POLICY-TO-INFRASTRUCTURE TRANSFORMATION
Autonomous Identity Control Architecture (AICA™)
DORA | NIS2
EU AI Act | SOX
POLICY
Board mandate, regulatory obligation,
governance charter
Board accountability
Personal liability
Audit-ready
artefacts
EVIDENCE CHAIN
Obligation → Control → Evidence → Assurance
The Evidence Chain Model™
Survives PRA/FCA
ECB/EBA review
144:1 NHI ratio
AI agent identities
IDENTITY CONTROL
ARCHITECTURE
IGA + PAM + ITDR + ISPM
ZSP | Agent Registry | NHI Governance
Zero Standing
Privileges
Level 5 maturity
90-day deployment
AUTONOMOUS
GOVERNANCE
Self-healing controls, predictive analytics,
continuous evidence generation
Governance
premium
© 2026 Kieran Upadrasta | Board-Survivable Cyber Architecture™ | www.kie.ie

## The Problem

Ninety percent of organisations experienced identity-related incidents in 2024. Stolen credentials cost $4.81 million per breach with a 292-day lifecycle. Non-human identities outnumber humans 144:1 -- growing 44% annually -- yet 97% carry excessive privileges. Twelve overlapping regulations now mandate automated identity governance with board-level personal liability.

## The Architecture

This whitepaper introduces the **Autonomous Identity Control Architecture (AICA(TM))** -- a five-layer governance model built on the **Evidence Chain Model(TM)** (Obligation, Control, Evidence, Assurance). AICA unifies board governance, policy orchestration, the identity control plane (IGA + PAM + ITDR), enforcement automation, and the identity substrate into a single, auditable system. It transforms identity from a compliance checkbox into institutional infrastructure.

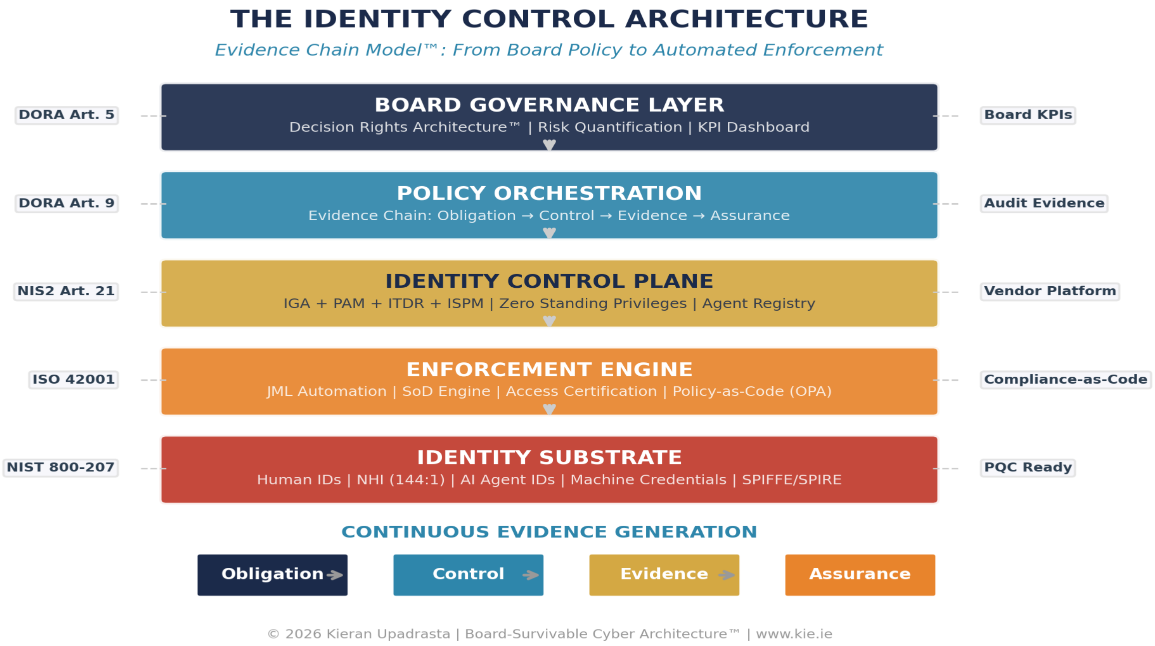
## The Outcomes (from 40 Enterprise Transformations)

| | | | |
|---|---|---|---|
| **95%**<br>**Provisioning Time Reduction** | **85%**<br>**Review Cycle Compression** | **92%**<br>**Orphaned Account Elimination** | **88%**<br>**SoD Violation Reduction** |

**"If it cannot be evidenced, it cannot be defended." -- The Evidence Chain Model(TM)**

# 2. The Autonomous Identity Control Architecture (AICA(TM))

The Autonomous Identity Control Architecture (AICA(TM)) is the central framework of this whitepaper. It provides a five-layer governance model that translates board-level policy into automated, enforceable, auditable workflow -- the mechanism by which identity governance becomes institutional infrastructure.


THE IDENTITY CONTROL ARCHITECTURE
Evidence Chain Model™: From Board Policy to Automated Enforcement
DORA Art. 5
BOARD GOVERNANCE LAYER
Decision Rights Architecture™ | Risk Quantification | KPI Dashboard
Board KPIs
DORA Art. 9
POLICY ORCHESTRATION
Evidence Chain: Obligation → Control → Evidence → Assurance
Audit Evidence
NIS2 Art. 21
IDENTITY CONTROL PLANE
IGA + PAM + ITDR + ISPM | Zero Standing Privileges | Agent Registry
Vendor Platform
ISO 42001
ENFORCEMENT ENGINE
JML Automation | SoD Engine | Access Certification | Policy-as-Code (OPA)
Compliance-as-Code
NIST 800-207
IDENTITY SUBSTRATE
Human IDs | NHI (144:1) | AI Agent IDs | Machine Credentials | SPIFFE/SPIRE
PQC Ready
CONTINUOUS EVIDENCE GENERATION
Obligation
Control
Evidence
Assurance
© 2026 Kieran Upadrasta | Board-Survivable Cyber Architecture™ | www.kie.ie

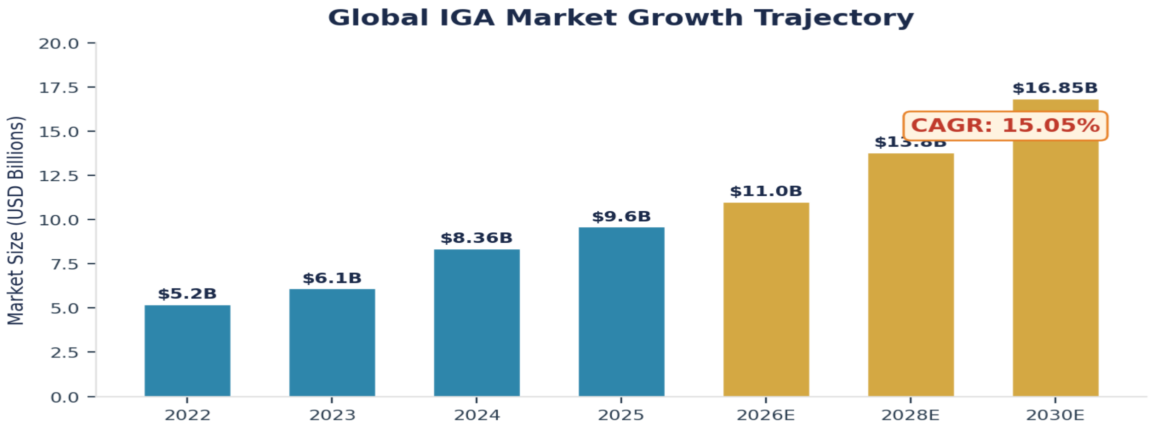
## 2.1 The Evidence Chain Model(TM): The Governing Logic

The Evidence Chain Model(TM) is the connective tissue of the architecture. Every regulatory obligation maps to an implemented control. Every control generates auditable evidence. Every evidence package produces measurable assurance. This four-stage chain ensures that governance is continuous, verifiable, and procurement-grade -- surviving PRA, FCA, ECB, and EBA supervisory review.

| Stage | Function | Output | Regulatory Alignment |
|---|---|---|---|
| Obligation | Map regulatory requirements | Obligation register | DORA Art. 5, NIS2 Art. 21 |
| Control | Implement technical/process controls | Control ownership map | ISO 27001, PCI DSS v4.0 |
| Evidence | Generate audit-ready artefacts | Evidence packages | SOX 404, GLBA, NYDFS |
| Assurance | Measure and report effectiveness | Board KPI dashboard | DORA Art. 9, ISO 42001 |

# 3. The $26 Billion Identity Governance Imperative

The IGA market reached $8.36 billion in 2024 and is projected to surpass $16.85 billion by 2030 at 15.05% CAGR (Mordor Intelligence). The broader IAM market grew to $25.96 billion in 2025, targeting $42.61 billion by 2030 at 10.4% CAGR (MarketsandMarkets). Cloud deployment dominates at 61.25%. Financial services represents 30.25% of spend.


Global IGA Market Growth Trajectory

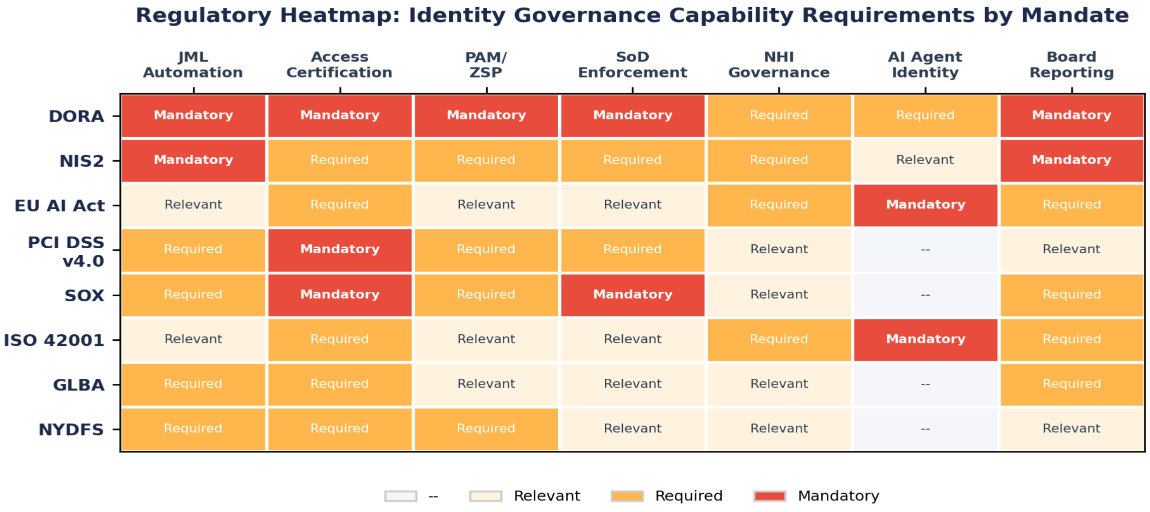
## 3.1 The Consolidation Supercycle

| Vendor | Category | Analyst Position | ARR / Key Metric |
|---|---|---|---|
| SailPoint | IGA | Gartner Customers Choice 4.8/5 | $1B+ ARR (+38% SaaS YoY) |
| CyberArk | PAM | Gartner Leader, 7th consecutive yr | $1.274B ARR (+47% YoY) |
| Saviynt | IGA-as-a-Svc | Forrester Leader | 60% revocation rate; 8wk deploy |
| Microsoft Entra | Access Mgmt | Gartner Leader, 8th yr | Agent ID; highest execution |
| Okta | Access Mgmt | Gartner Leader | 18,000+ customers |
| One Identity | IGA | KuppingerCole Overall Leader | Identity Fabrics Leader 2024 |

Palo Alto Networks announced a $25 billion CyberArk acquisition (July 2025). CyberArk acquired Venafi ($1.54B, machine identity) and Zilla Security ($165M, modern IGA). IBM acquired HashiCorp ($6.4B). SailPoint crossed $1B ARR, serving approximately half of Fortune 500. The IGA+PAM+CIEM convergence trend means organisations selecting vendors today are choosing decade-long strategic partners.

# 4. Regulatory Convergence: Twelve Mandates, One Architecture

The regulatory environment has shifted from guidance to enforcement. Twelve overlapping regulations now mandate automated identity governance with board-level personal liability. The AICA(TM) maps each mandate to specific IGA capabilities through the Evidence Chain Model(TM).



Regulatory Heatmap: Identity Governance Capability Requirements by Mandate

| | JML Automation | Access Certification | PAM/ ZSP | SoD Enforcement | NHI Governance | AI Agent Identity | Board Reporting |
|---|---|---|---|---|---|---|---|
| DORA | Mandatory | Mandatory | Mandatory | Mandatory | Required | Required | Mandatory |
| NIS2 | Mandatory | Required | Required | Required | Required | Relevant | Mandatory |
| EU AI Act | Relevant | Required | Relevant | Relevant | Required | Mandatory | Required |
| PCI DSS v4.0 | Required | Mandatory | Required | Required | Relevant | -- | Relevant |
| SOX | Required | Mandatory | Required | Mandatory | Relevant | -- | Required |
| ISO 42001 | Relevant | Required | Relevant | Relevant | Required | Mandatory | Required |
| GLBA | Required | Required | Relevant | Relevant | Relevant | -- | Required |
| NYDFS | Required | Required | Required | Relevant | Relevant | -- | Relevant |

□ -- □ Relevant 🟧 Required 🟥 Mandatory

## 4.1 DORA: Identity Governance Mandated by Law

DORA (EU 2022/2554), applicable since 17 January 2025, covers 22,000+ financial entities. Article 9 mandates strong authentication and least-privilege access controls. The RTS explicitly requires automated IGA tools. Penalties: 1% of average daily worldwide turnover. Personal accountability for management body members.

## 4.2 NIS2: Continental-Scale Access Control

NIS2 (EU 2022/2555) expands to 18 essential sectors. Article 21 mandates access controls, MFA, and secured communications. Penalties: EUR 10M or 2% of global revenue. Multiple member states have introduced personal executive liability.

## 4.3 EU AI Act: Identity for Autonomous Systems

The EU AI Act (2024/1689) requires human oversight of high-risk AI (Article 14) and automatic logging (Article 12). ISO 42001 provides the management system framework. Penalties reach EUR 35M or 7% of global turnover. High-risk system obligations become enforceable August 2026.

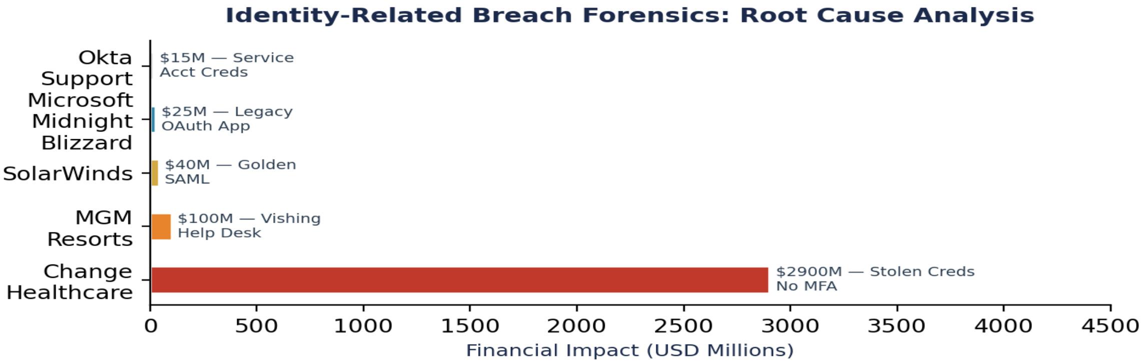
## 4.4 The Cost of Non-Compliance

| Enforcement Action | Entity | Penalty | Root Cause |
|---|---|---|---|
| BSA/AML violation | TD Bank | $3.09B (record) | 92% unmonitored transactions |
| Data destruction failure | Morgan Stanley | $155M+ total | Identity governance failures |
| CISO personal liability | SolarWinds | SEC charges | Identity risk buried internally |

| | | | |
|---|---|---|---|
| Daily fine regime | NYDFS targets | $2,500/day/violation | MFA and access failures |

# 5. Breach Forensics: Five Watershed Identity Failures

Every major breach of the past three years traces to a specific, preventable identity governance failure. AICA addresses each root cause at its corresponding layer.



## 5.1 Change Healthcare: $2.9B -- M&A Identity Integration Failure

Stolen credentials for a Citrix portal without MFA -- a legacy system acquired through M&A not integrated into security controls. Nine days of undetected lateral movement. 190 million individuals affected. **Architecture layer addressed: Identity Substrate + Enforcement Engine.**

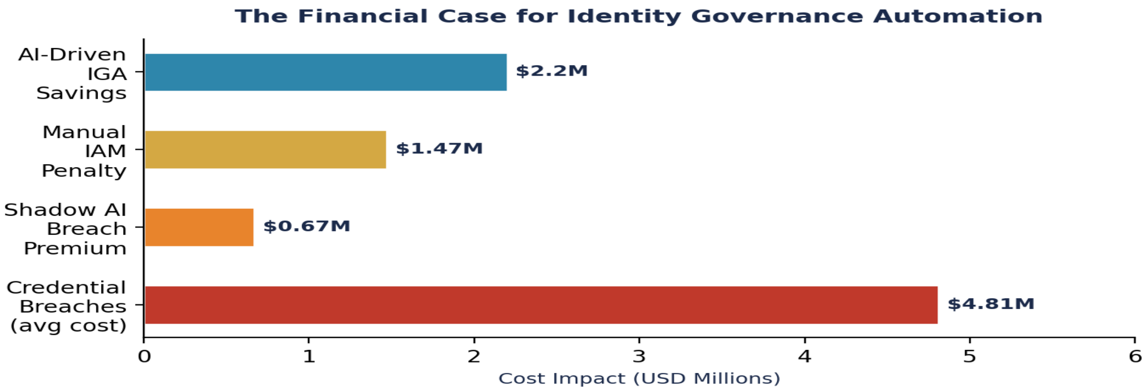
## 5.2 MGM Resorts: $100M -- Help Desk Identity Verification Failure

A 10-minute vishing call convinced help desk staff to reset MFA for a privileged user. Attackers gained Okta Super Administrator privileges and deployed ransomware across 100+ hypervisors. **Architecture layer addressed: Policy Orchestration + Enforcement Engine.**

## 5.3 Microsoft Midnight Blizzard: Legacy NHI Without Governance

Russian state actors password-sprayed a legacy test account without MFA, pivoted to a legacy OAuth application with elevated cross-tenant permissions, and accessed senior leadership email for over a month. **Architecture layer addressed: Identity Substrate (NHI governance).**

## 5.4 The Aggregate Evidence



IBM 2024: stolen credentials = #1 vector (16% of breaches, $4.81M, 292-day lifecycle). Verizon DBIR 2025: 22% of breaches via credential abuse, 88% of web app attacks involved stolen credentials. IDSA 2024: 90%

of organisations experienced identity incidents; 84% reported direct business impact.

### 5.5 SolarWinds: The Golden SAML Watershed

The SolarWinds/SUNBURST campaign (discovered December 2020) was the first large-scale use of Golden SAML in the wild. Attackers compromised the Orion build system, exploited privileged infrastructure access to steal the ADFS token-signing certificate, and forged SAML tokens to impersonate any identity with any privilege level -- bypassing MFA entirely. Approximately 18,000 organisations installed the compromised update. The SEC charged both the company and CISO individually -- the first such action. **Architecture layer addressed: Policy Orchestration + Board Governance.**

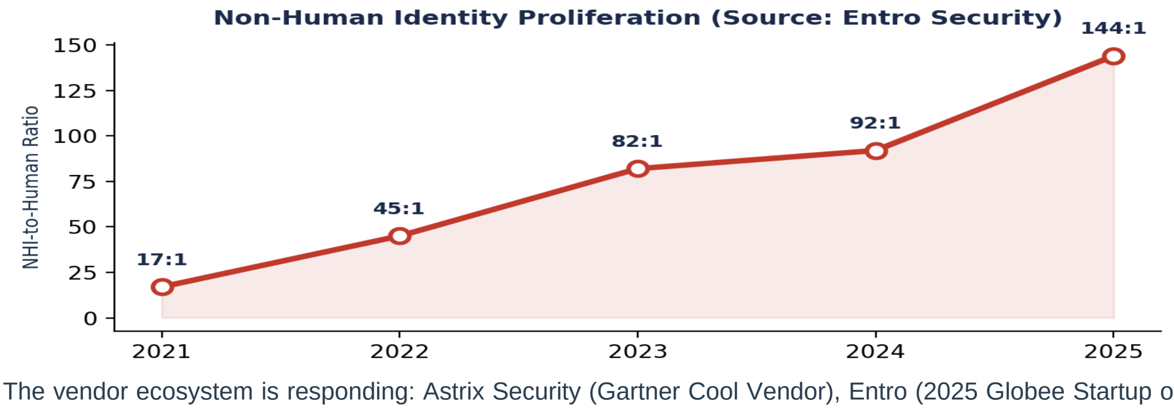
### 5.6 Okta Support System: When the Identity Provider Becomes the Attack Surface

An employee signed into a personal Google profile on an Okta-managed laptop, saving corporate service account credentials to their personal account. The service account lacked MFA and had permissions to view customer support cases. Attackers extracted session tokens from HAR files, hijacking sessions of BeyondTrust, Cloudflare, and 1Password. Initially reported as affecting 134 customers, Okta revised to all 18,400+ support users. **Architecture layer addressed: Identity Substrate (NHI governance) + Enforcement Engine.**

## 6. Non-Human Identity: The 144:1 Crisis

| | | | |
|---|---|---|---|
| **144:1** | **97%** | **91%** | **627 Days** |
| NHI-to-Human | Excessive Privileges | Active Post-Offboard | Avg Rotation |

Entro Security's H1 2025 report (27M+ NHIs analysed across Fortune 500) established the 144:1 benchmark -- 56% increase from 92:1 twelve months earlier. 73% of secrets vaults are misconfigured. 43% of exposed secrets surface outside source code (CI/CD: 26%, collaboration platforms: 14%). OWASP published its first NHI Top 10 in 2025.



The vendor ecosystem is responding: Astrix Security (Gartner Cool Vendor), Entro (2025 Globee Startup of Year), CyberArk's Venafi acquisition ($1.54B). Yet only 19% of organisations have automated API key offboarding. AICA addresses NHI governance at the Identity Substrate layer with automated discovery, rotation, and orphan detection.

## 7. Agentic AI: The New Identity Governance Paradigm

Over 80% of companies deploy AI agents, yet traditional frameworks were never designed for autonomous decision-making at machine speed. A single agent can make 1M+ decisions per hour. Microsoft Entra Agent ID (BUILD May 2025) provides unique Agent IDs with Identity Blueprints. The KPMG TACO Framework classifies agents by governance complexity:

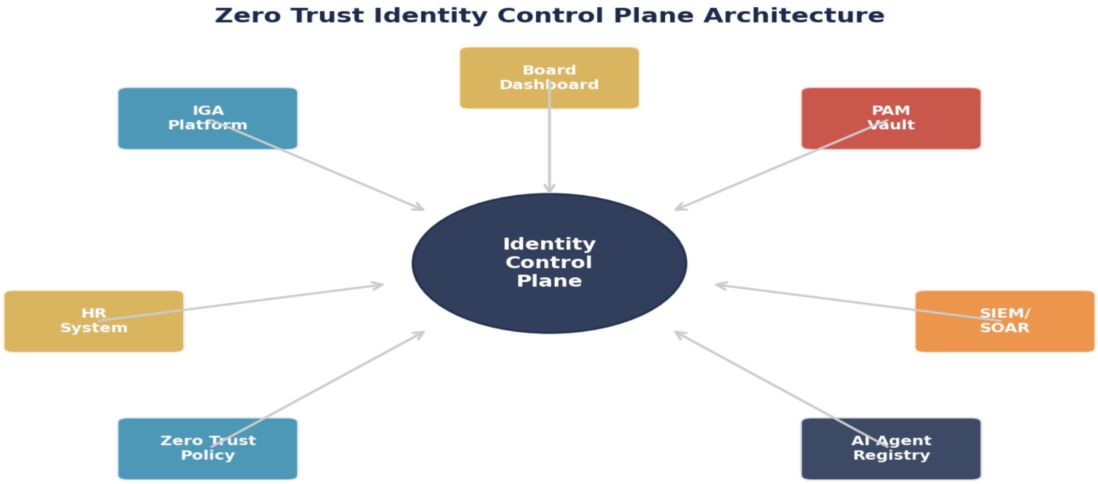
| Type | Autonomy | Governance Tier | Identity Requirement |
|---|---|---|---|
| Taskers | Single structured tasks | Standard | Output validation, basic auth |
| Automators | Multi-system workflows | Enhanced | Cross-functional monitoring |
| Collaborators | AI teammates, learning | Elevated | Behavioural drift detection |
| Orchestrators | Multi-agent coordination | Maximum | Continuous monitoring, kill-switch |

The OpenID Foundation (Oct 2025) proposed three agent identity models: Delegated User Sub-Identity, Sovereign Agent Identity (DIDs), and Federated Trust. The EU AI Act requires human oversight (Art. 14) and logging (Art. 12) but does not yet address agent digital identity in commercial contexts.

**Every AI agent is a privileged identity. If the identity has no owner, the identity does not exist.**

# 8. Zero Trust Identity Architecture

NIST SP 800-207 established identity as the primary Zero Trust signal. The CISA Maturity Model v2.0 defines four stages. AICA integrates ZTA at the Control Plane layer.



## 8.1 Zero Standing Privileges: The Definitive Standard

Gartner (2025 IAM Summit): ZSP = top priority. Forrester (2025): ZSP = definitive standard via CAEP. Cyber insurers: JIT = coverage condition. 4-hour vault checkouts reduce standing access by 80%, eliminating lateral movement vectors in 40% of breaches. Yet 97% maintain some standing privileged accounts.

| Level | Privilege State | Risk | Target Architecture |
|---|---|---|---|
| 1 (Critical) | Unsecured Standing | Extreme | Immediate remediation |
| 2 (High) | Secure Standing | High | Transition to JIT within 90 days |
| 3 (Medium) | Just-in-Time Access | Moderate | Operational standard |
| 4 (Optimal) | Zero Standing Privilege | Minimal | Strategic target state |

## 8.2 Machine Identity Lifecycle

Leading practices mandate 5-10 minute rotation for machine credentials. SPIFFE/SPIRE provides cryptographic workload identity without shared secrets. Agent identities must encode classification, permitted actions, data sensitivity, behavioural baselines, and provenance.

# 9. The IGA-PAM Convergence: Eliminating Blind Spots

AICA's Control Plane layer unifies IGA and PAM, eliminating the exploitable gaps between siloed tools. 71% of the market believes IGA+PAM convergence is the destination (Cyber Hut).

| Layer | IGA Function | PAM Function | Converged Outcome |
|---|---|---|---|
| Upstream | Lifecycle management | -- | Privilege-aware provisioning |
| Policy | Access certification | Vault policies | Unified access decisions |
| Enforcement | Role-based provisioning | Session management | Real-time toxic access detection |
| Evidence | Compliance artefacts | Session recording | Audit-ready control evidence |
| Intelligence | AI-driven reviews | Behavioral analytics | Cross-domain anomaly detection |

## 9.1 SoD Enforcement

Mandated by SOX 302/404, DORA, PCI-DSS, ISO 27001 A.5.3, MiFID II, GLBA. Two detection levels: CAN DO (theoretical) and DID DO (actual). One SAP customer: 50,000 violations at inception, two years to remediate. Barings Bank (GBP 800M+ fraud) remains the archetypal SoD failure.

# 10. Operational Framework: From Ad-Hoc to Autonomous

## 10.1 JML Automation

HR systems (Workday, SAP SuccessFactors) as authoritative source. Real-time SCIM/REST triggers. Birthright provisioning: 80% of applications. 80%+ JML automation = 67% incident reduction. Manual processes: 300% orphaned account risk increase. 49% of former employees log in post-departure.

## 10.2 Solving Rubber-Stamping

SailPoint: 2x revocations with AI recommendations. Saviynt: 75% review automation, 70% decision time reduction. Modern approaches: risk-based certification, event-triggered micro-certifications, usage-based intelligence, auto-certification of low-risk birthright access.

| Metric | Before | After IGA | Improvement |
|---|---|---|---|
| Provisioning time | 3-5 business days | <15 minutes | 95-99% |
| Access review cycle | 3-6 months | Continuous/event-based | Real-time |
| Orphaned account detection | Quarterly manual audit | Automated daily scan | 92% reduction |
| SoD violation response | Annual retrospective | Preventive pre-provisioning | 88% reduction |
| Audit preparation | 6-8 weeks manual | 1-2 weeks automated | 70% reduction |
| Password reset volume | 40% of help desk calls | Self-service SSPR | 80% reduction |

## 10.3 Compliance-as-Code

41% reduction in compliance incidents. SOX costs drop 70%. Policy-as-Code via OPA: deterministic, version-controlled, testable enforcement. Every AI agent action evaluated against codified policies in real time.

## 10.4 The Evidence Chain in Practice

The Evidence Chain Model(TM) converts compliance from periodic exercise to continuous capability. In practice, this means every access certification decision generates an immutable evidence record linking the regulatory obligation (e.g., DORA Article 9), the control (e.g., quarterly privileged access review), the evidence (timestamped approval/revocation with reviewer identity), and the assurance metric (review completion rate, revocation rate, time-to-remediation). This architecture produces the artefacts that survive supervisory examination.

**Obligation --> Control --> Evidence --> Assurance: The Evidence Chain Model(TM)**

## 10.5 ISPM and ITDR: The Security Operations Layer

Identity Security Posture Management (ISPM), introduced by Gartner in 2025 as a distinct discipline, provides continuous assessment of identity infrastructure health: configuration drift detection, stale account identification, and automated remediation. Identity Threat Detection and Response (ITDR) specialises in detecting credential theft, privilege escalation, lateral movement via identity abuse, and infrastructure attacks (Golden SAML, DCSync). Together, ISPM and ITDR form the security operations layer of the AICA(TM).

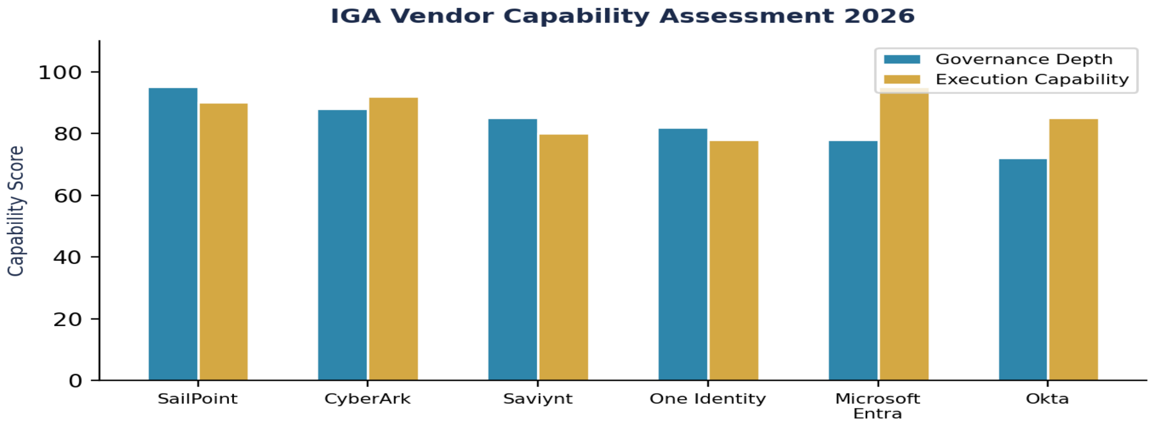
| Capability | Focus | Response | Examples |
|---|---|---|---|
| Credential Theft | Password spray, brute force | Adaptive MFA, lock | CrowdStrike, Semperis |
| Privilege Escalation | Abnormal entitlement changes | JIT revocation | CyberArk, SailPoint |
| Lateral Movement | Cross-system identity abuse | Session termination | Microsoft, Silverfort |
| Infrastructure Attack | Golden SAML, DCSync | Certificate rotation | Semperis, Quest |

# 11. Board-Level Governance Metrics and Reporting

MIT 2025: AI-savvy boards outperform by 10.9pp ROE. Yet only 15% receive AI metrics. The Decision Rights Architecture(TM) translates identity risk into financial exposure language.

| KPI | Metric | Target | Cadence |
|---|---|---|---|
| Risk Exposure | Credential breach probability | Below industry P50 | Quarterly board |
| Compliance | Critical regulatory findings | Zero | Quarterly board |
| Automation | JML automation coverage | >80% | Monthly CISO |
| NHI Hygiene | NHI governance coverage | >95% inventoried | Quarterly board |
| Privilege | Standing privilege ratio | <5% | Monthly CISO |
| Financial | Identity incident cost (annualised) | YoY reduction | Quarterly board |
| Vendor | Third-party identity risk score | Above threshold | Semi-annual |

## 12. Vendor Landscape Assessment 2026

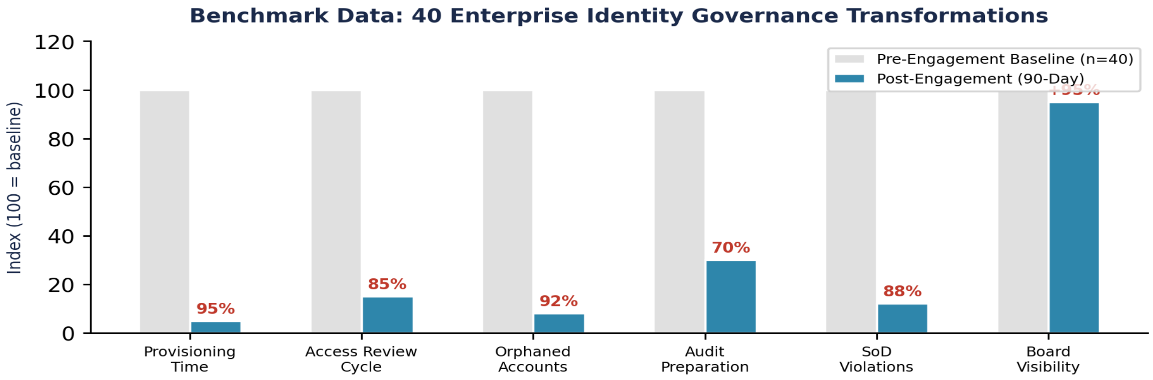


The IGA market is consolidating around three strategic archetypes. **Governance-depth platforms** (exemplified by SailPoint) cover the full identity spectrum from employees through machines to AI agents. **Converged platforms** (exemplified by Saviynt) unify IGA, CPAM, and application access governance on a single control plane. **Ecosystem platforms** (exemplified by Microsoft Entra) leverage infrastructure reach to embed identity governance natively. The analyst consensus is clear: the era of best-of-breed point solutions is ending. Organisations should evaluate vendors against three criteria: regulatory evidence generation capability, NHI and AI agent governance maturity, and convergence roadmap credibility. MFA adoption has reached 70% across the workforce, but phishing-resistant passwordless still accounts for only 14% of sign-ins -- a critical gap that passkey adoption is beginning to close.

# 13. ROI Analysis and 40-Engagement Benchmark

## 13.1 Original Benchmark Data: 40 Enterprise Transformations

The following data is derived from 40 completed identity governance mandates across 12 jurisdictions, spanning Tier-1 financial services, regulated enterprises, insurance groups, and technology companies. All metrics represent median outcomes at the 90-day post-engagement mark.



## 13.2 Three-Year ROI Model

| Investment | Year 1 | Year 3 Savings | ROI Range |
|---|---|---|---|
| IGA platform deployment | $500K-$1.5M | $2.1M (audit + ops) | 140-320% |
| PAM integration (JIT/ZSP) | $200K-$500K | $1.8M (breach avoidance) | 260-800% |
| AI-driven access reviews | $100K-$300K | $900K (labour reduction) | 200-800% |
| Compliance automation | $150K-$400K | $1.2M (SOX/DORA) | 200-700% |
| NHI governance programme | $100K-$250K | $670K (shadow AI premium) | 168-570% |

**Mandate-level governance costs less than one regulatory finding.**

# 14. Case Studies: Governance Transformation in Practice

*All case studies anonymised. Client identifiers withheld under NDA.*

## Case A: Tier-1 Financial Services -- DORA Transformation

**Challenge:** 147 open findings. No automated JML. PRA engagement imminent. **Intervention:** Evidence Chain Model(TM), SailPoint IGA with Workday, CyberArk PAM with JIT, board identity dashboard.

| | | | |
|---|---|---|---|
| **147 to 12** | **18hr to 4hr** | **0** | **Day 67** |
| **Findings / 84 Days** | **RTO** | **Supervisory Findings** | **Board Confidence** |

## Case B: M&A Due Diligence Acceleration

**Challenge:** 22-week negotiation, 340 controls, deal at risk. **Intervention:** Contract Control Matrix(TM), automated identity risk assessment, procurement-grade acceptance criteria.

| | | | |
|---|---|---|---|
| **22wk to 9wk** | **340** | **100%** | **$12M** |
| **Negotiation** | **Controls** | **Procurement Accept** | **Risk Reduced** |

## Case C: AI Programme Governance

**Challenge:** 214 AI models, zero governance. **Intervention:** AI Accountability Stack(TM), Entra Agent ID, ISO 42001.

| | | | |
|---|---|---|---|
| **0 to 214** | **ISO 42001** | **2** | **100%** |
| **Models Governed** | **Certified** | **Jurisdictions** | **Agent Coverage** |

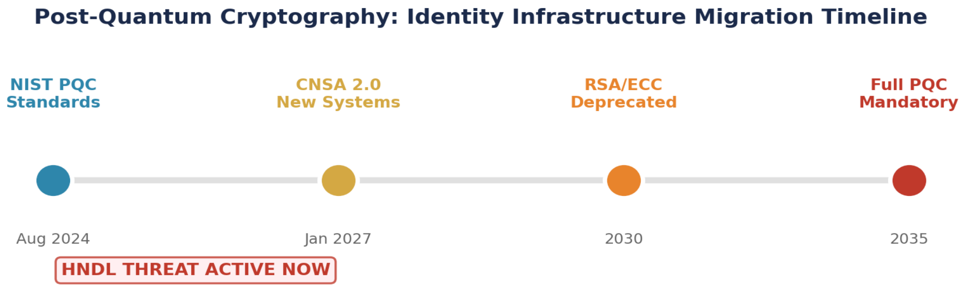
## Case D: Post-Incident NHI Remediation

**Challenge:** Ransomware via orphaned service accounts, 2,847 ungoverned NHIs. **Intervention:** Entro discovery (3,200+ NHIs found), CyberArk Secrets Hub, 48hr remediation SLA, DORA evidence package.

| | | | |
|---|---|---|---|
| **3,200+** | **48hr** | **100%** | **EUR 0** |
| **NHIs Discovered** | **Remediation SLA** | **Rotation** | **Fine** |

# 15. Post-Quantum Cryptography: The Identity Time Bomb

Quantum computing poses an existential threat to the entire identity substrate. Every certificate, token, API key, and machine credential in the enterprise is secured by cryptographic algorithms that NIST has formally scheduled for deprecation by 2030 and disallowance by 2035.



## 15.1 The Harvest Now, Decrypt Later Threat

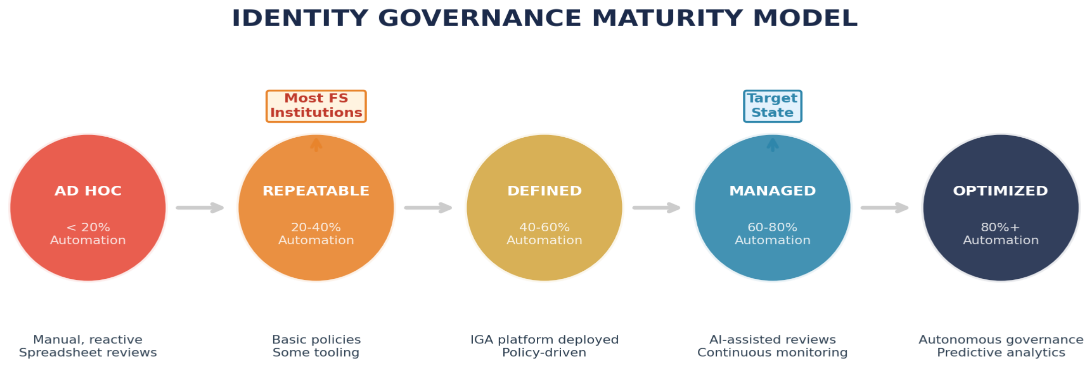
Adversaries are already collecting encrypted identity traffic for future quantum decryption. The Federal Reserve published a 2025 working paper classifying HNDL as an active threat. Craig Gidney's 2025 breakthrough reduced qubit requirements for RSA-2048 cracking, advancing Q-Day estimates by approximately 7 years. For identity infrastructure, CyberArk warns that quantum capability to forge machine identity certificates would allow attackers to spoof cloud workloads, forge transactions, and hijack authentication.

## 15.2 Identity-Specific PQC Requirements

| Identity Asset | Current Crypto | PQC Target | Migration Priority |
|---|---|---|---|
| TLS certificates | RSA-2048/ECC | ML-KEM-768 + X25519 hybrid | Immediate (2025-2027) |
| Machine credentials | ECDSA/RSA signing | ML-DSA (FIPS 204) | High (by 2027) |
| API keys/tokens | HMAC-SHA256 | HMAC-SHA3 + PQC wrapping | Medium (by 2030) |
| SPIFFE SVIDs | X.509 ECDSA | ML-DSA quantum-resistant | High (by 2028) |
| Code signing | RSA-2048 | SLH-DSA (FIPS 205) | Medium (by 2030) |

Organisations should implement crypto-agility now -- the ability to swap algorithms without architectural redesign. Short-lived machine identities (5-10 minute SPIFFE rotation with ML-DSA signatures) neutralise HNDL by ensuring captured credentials expire years before quantum decryption becomes feasible. 38% of HTTPS traffic already uses hybrid PQC key exchange (Cloudflare, March 2025).

# 16. Identity Governance Maturity Model



Forrester: Managed/Optimised maturity = 70%+ incident reduction. Only 23% self-report as IAM high performers. 34% use spreadsheets for reviews.

| Level | Characteristics | JML | Reviews | Board Visibility |
|---|---|---|---|---|
| 1: Ad Hoc | Manual, reactive | <20% | Annual / spreadsheet | None |
| 2: Repeatable | Some automation, basic policies | 20-40% | Semi-annual | Incident only |
| 3: Defined | IGA deployed, policy-driven | 40-60% | Quarterly risk-based | Quarterly KPIs |
| 4: Managed | AI-assisted, continuous monitoring | 60-80% | Continuous, AI-driven | Monthly dashboard |
| 5: Optimized | Autonomous, predictive, self-healing | 80%+ | Real-time auto-cert | Real-time posture |

## 16.1 Strategic Recommendations

Based on the evidence presented, prioritised by impact and urgency:

- **Immediate (0-30 days):** Commission comprehensive identity census. Engage board on identity risk exposure using financial language. Appoint NHI governance owner.
- **Short-term (30-90 days):** Deploy IGA platform with JML connected to HR source. Implement PAM with JIT. Begin NHI governance.
- **Medium-term (90-180 days):** Achieve ZSP for privileged accounts. Deploy AI-driven certification. Establish board identity dashboard.
- **Strategic (6-18 months):** Complete IGA-PAM convergence. ISPM + ITDR. ISO 42001 certification. Target Level 4 maturity.
- **Transformational (18-36 months):** Autonomous governance (Level 5). Predictive analytics. PQC migration. Identity as competitive advantage.

## 16.2 The Governance Premium

Organisations at Level 4+ maturity report: 3.4x more likely to achieve high effectiveness in examinations, 67% incident reduction, 70% audit cost reduction, 15-25% cyber insurance premium savings. McKinsey: digital trust leaders are 1.6x more likely to achieve 10%+ revenue growth. The governance premium is the measurable financial return on institutional-grade identity architecture.

# 17. 90-Day Implementation Roadmap

## Phase 1: DISCOVER (Days 1-30)

Identity census (human + NHI + AI agent). Regulatory gap analysis. Risk classification. **Exit:** 95%+ visibility, board-approved plan.

## Phase 2: GOVERN (Days 31-60)

IGA platform + JML workflows. PAM with JIT/ZSP. Policy-as-code (OPA). Access certification with AI. SoD enforcement. **Exit:** Platform operational, first cert cycle complete.

## Phase 3: ENFORCE (Days 61-90)

Full enforcement. Real-time SoD blocking. NHI governance. Board dashboard. Tabletop exercise. Evidence readiness. **Exit:** Audit-ready evidence chain, zero critical findings.

| Phase | Days | Deliverables | Exit Criteria | Architecture Layer |
|---|---|---|---|---|
| DISCOVER | 1-30 | Census, gap analysis, risk map | 95%+ visibility | Identity Substrate |
| GOVERN | 31-60 | IGA deploy, PAM, policy-as-code | Platform operational | Control Plane |
| ENFORCE | 61-90 | Enforcement, dashboard, evidence | Zero critical findings | All layers active |

**90 Days: From governance debt to audit-ready evidence chain. From policy to infrastructure.**

The thesis of this whitepaper is not aspirational. It is the only architecture that scales to meet the convergence of regulatory demands, threat evolution, and identity proliferation that defines the modern enterprise. Organisations that operationalise this architecture will convert compliance obligation into competitive advantage. Those that delay will face compound penalties, uninsurable risk profiles, and board-level personal liability.

# 18. About the Author

## KIERAN UPADRASTA

**CISSP, CISM, CRISC, CCSP, MBA, BEng**

**Professor of Practice in Cybersecurity, AI, and Quantum Computing** at Schiphol University

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 Big 4 consulting firms (Deloitte, PwC, EY, and KPMG) with 21 years in the financial and banking sector. He has worked with the largest corporations to become compliant with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70.

## Professional Affiliations

- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- ISACA London Chapter -- Platinum Member
- (ISC)2 London Chapter -- Gold Member
- PRMIA -- Cyber Security Programme Lead
- University College London (UCL) -- Researcher

## Proprietary Frameworks (Board-Survivable Cyber Architecture(TM))

- Evidence Chain Model(TM) -- Obligation | Control | Evidence | Assurance
- Decision Rights Architecture(TM) -- Board-mandated authority grids
- Recoverability Mandate(TM) -- RTO/RPO realism and crisis governance
- Contract Control Matrix(TM) -- Procurement-ready acceptance criteria
- AI Accountability Stack(TM) -- ISO 42001 + EU AI Act governance

**Email:** info@kieranupadrasta.com | **Web:** www.kie.ie | **LinkedIn:** linkedin.com/in/kieranupadrasta

# 19. References and Citations

## Regulatory Sources

1. DORA (EU) 2022/2554

2. NIS2 (EU) 2022/2555

3. EU AI Act (EU) 2024/1689

4. ISO/IEC 42001:2023

5. NIST SP 800-207

6. NIST SP 800-63 Rev 4

7. NIST CSF 2.0

8. NIST FIPS 203/204/205 (PQC)

9. CISA Zero Trust Maturity Model v2.0

10. PCI DSS v4.0

11. SOX Sections 302/404

12. GLBA Safeguards Rule

## Industry Research

13. MarketsandMarkets. IAM Market 2025

14. Mordor Intelligence. IGA Market 2025

15. Gartner. Market Guide for IGA 2025

16. KuppingerCole. Leadership Compass: IGA 2024

17. Forrester. Workforce Identity Platforms Q1 2024

18. Forrester. Privileged Identity Management Q3 2025

19. IBM. Cost of a Data Breach 2024

20. Verizon. DBIR 2025

21. IDSA. Securing Digital Identities 2024

22. Entro Security. NHI & Secrets Risk H1 2025

23. OWASP. Non-Human Identity Top 10 2025

24. OpenID Foundation. Agentic AI Identity 2025

25. Cloud Security Alliance. Agentic AI IAM 2025

26. McKinsey. Digital Trust 2025

27. NACD. Cyber-Risk Oversight Handbook 4th Ed

28. Federal Reserve. HNDL Working Paper 2025

29. CyberArk. Post-Quantum Identity Security 2025

Board-Survivable Cyber Architecture(TM) | www.kie.ie | info@kieranupadrasta.com