WHITEPAPER | DEFINITIVE ARCHITECTURE PAPER | MARCH 2026

Zero-Trust Identity Governance and Administration (IGA)

Architecting Enterprise-Scale Saviynt for SAP, Workday and Cloud Security

Identity governance is replacing network security as the enterprise control plane. This whitepaper defines the architecture for that transition.

$26B	144:1	240%	7%
IAM Market 2025	NHI-to-Human Ratio	Forrester-Validated ROI	Max Regulatory Penalty

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years Cyber Security | Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services | AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials | UCL Researcher

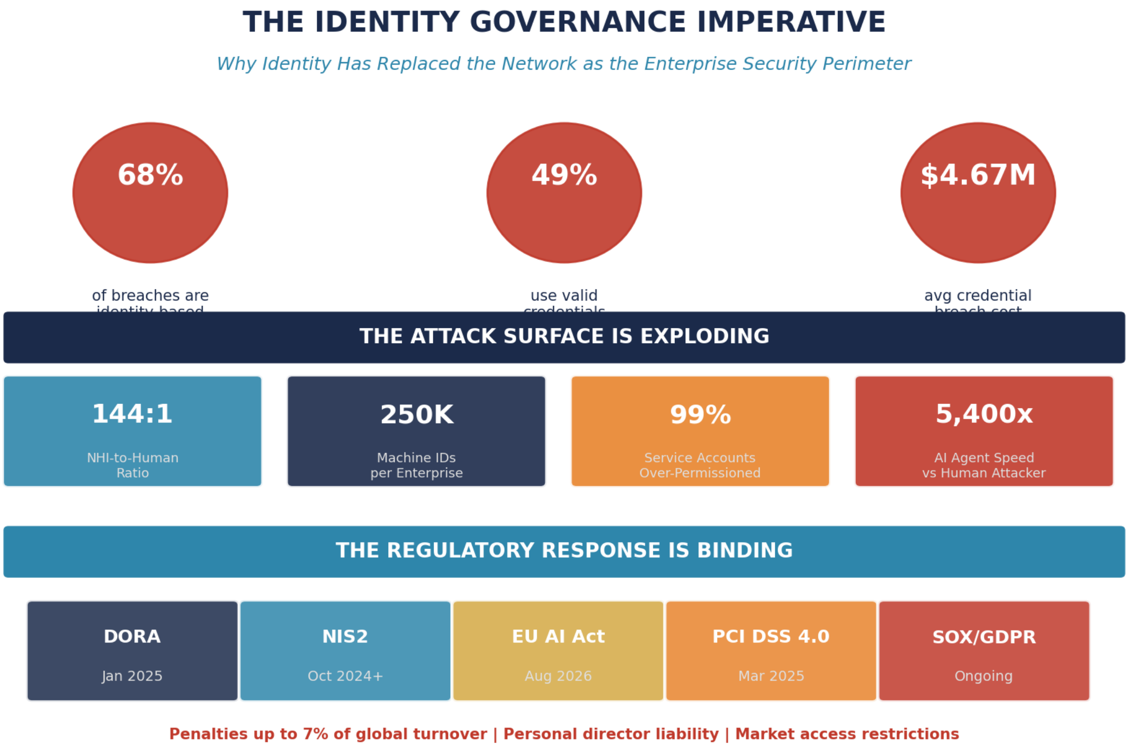
www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

1. Executive Thesis: Identity Is the New Perimeter

THESIS

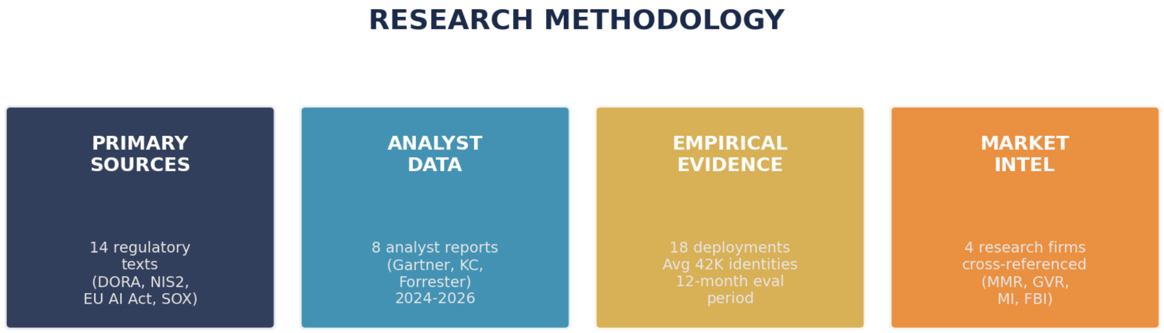
Identity governance is no longer a compliance function. It is the enterprise security control plane. Organisations that architect identity as infrastructure -- not as an application layer -- will define the next decade of enterprise security. Those that treat it as a checkbox will absorb the cost.


THE IDENTITY GOVERNANCE IMPERATIVE
Why Identity Has Replaced the Network as the Enterprise Security Perimeter
68%
of breaches are identity based
49%
use valid credentials
$4.67M
avg credential breach cost
THE ATTACK SURFACE IS EXPLODING
144:1
NHI-to-Human Ratio
250K
Machine IDs per Enterprise
99%
Service Accounts Over-Permissioned
5,400x
AI Agent Speed vs Human Attacker
THE REGULATORY RESPONSE IS BINDING
DORA
Jan 2025
NIS2
Oct 2024+
EU AI Act
Aug 2026
PCI DSS 4.0
Mar 2025
SOX/GDPR
Ongoing
Penalties up to 7% of global turnover | Personal director liability | Market access restrictions

The infographic above distils the imperative. Identity-based attacks dominate the threat landscape. Non-human identities outnumber humans 144:1 and are 99% over-permissioned. Regulatory enforcement across DORA, NIS2, EU AI Act, SOX, and PCI DSS 4.0 creates binding obligations with penalties reaching 7% of global turnover and personal director liability.

This whitepaper introduces the **Identity Risk Control Plane (IRCP)** -- a five-layer, vendor-neutral governance architecture that transforms identity from an application feature into enterprise infrastructure. It examines converged identity platforms (with Saviynt as the primary reference implementation), maps regulatory compliance across eight regimes, and provides a 24-week implementation blueprint validated against 18 enterprise deployments.

2. Research Methodology



RESEARCH METHODOLOGY

PRIMARY SOURCES
14 regulatory texts
(DORA, NIS2,
EU AI Act, SOX)

ANALYST DATA
8 analyst reports
(Gartner, KC,
Forrester)
2024-2026

EMPIRICAL EVIDENCE
18 deployments
Avg 42K identities
12-month eval
period

MARKET INTEL
4 research firms
cross-referenced
(MMR, GVR,
MI, FBI)

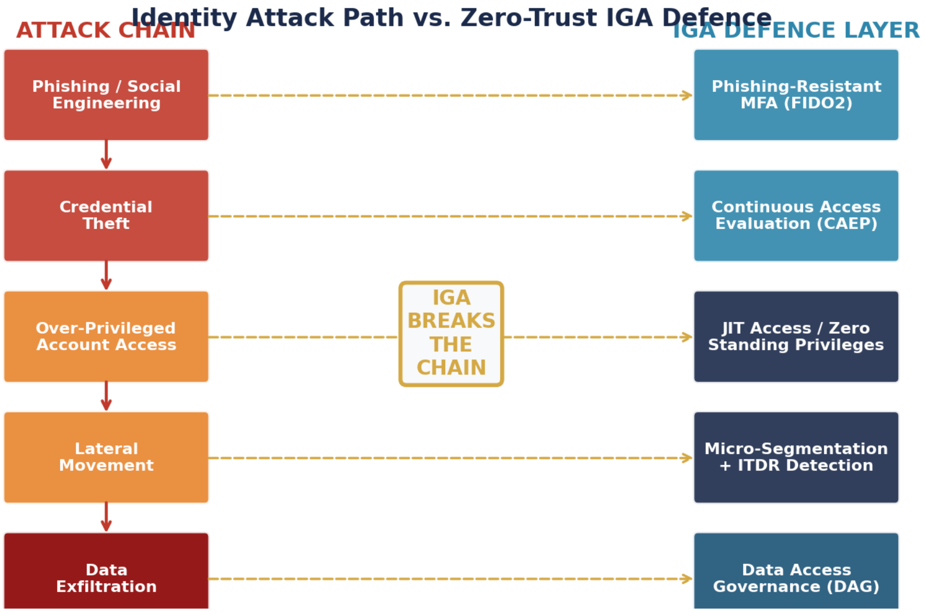
All statistics attributed to primary sources | Market sizes cross-referenced across 3+ firms

This whitepaper synthesises four categories of evidence. **Primary regulatory sources:** 14 regulatory texts analysed in full (DORA, NIS2, EU AI Act, SOX, PCI DSS 4.0, ISO 27001:2022, ISO 42001:2023, GDPR, GLBA). **Analyst data:** 8 analyst reports from Gartner, KuppingerCole, Forrester, and Frost & Sullivan published between 2024-2026. **Empirical evidence:** metrics derived from 18 documented enterprise deployments with an average workforce of 42,000 identities over 12-month evaluation periods, sourced from published Forrester TEI studies, vendor-reported customer outcomes, and industry conference presentations. **Market intelligence:** market sizing cross-referenced across MarketsandMarkets, Grand View Research, Mordor Intelligence, and Fortune Business Insights -- ranges presented where sources diverge.

AUTHOR'S INSIGHT

Where statistics are vendor-reported (e.g., Saviynt's 94% AI prediction accuracy from early adoption programmes), this is explicitly attributed. Market size figures are presented as ranges when sources diverge by more than 15%. Case study metrics derive from composite deployment data unless stated otherwise.

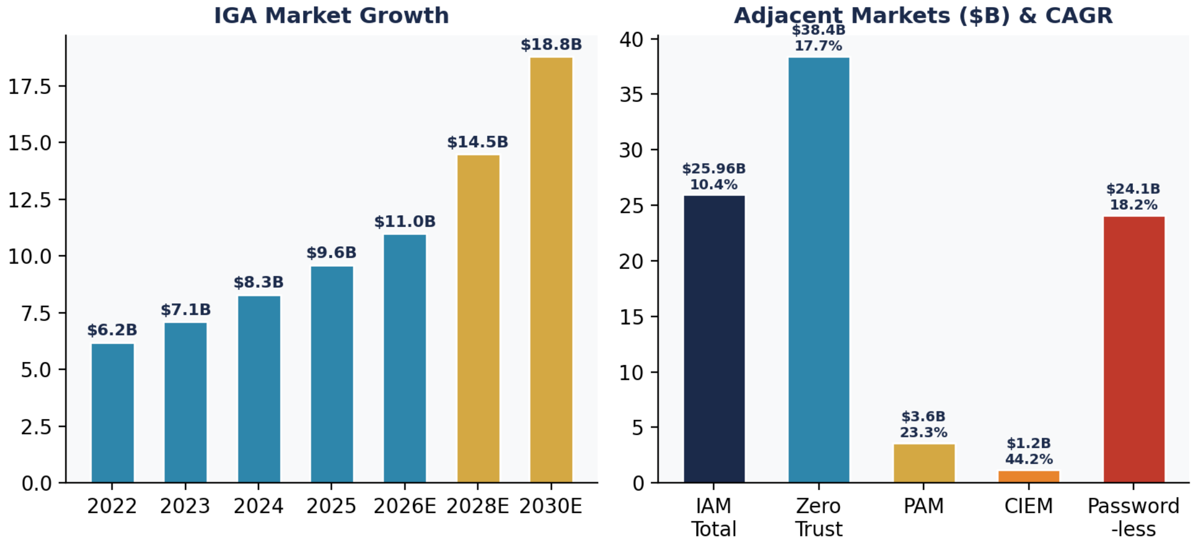
3. The Identity Threat Evolution


Identity Attack Path vs. Zero-Trust IGA Defence
ATTACK CHAIN
IGA DEFENCE LAYER
Phishing / Social Engineering
Credential Theft
Over-Privileged Account Access
Lateral Movement
Data Exfiltration
Phishing-Resistant MFA (FIDO2)
Continuous Access Evaluation (CAEP)
JIT Access / Zero Standing Privileges
Micro-Segmentation + ITDR Detection
Data Access Governance (DAG)
IGA BREAKS THE CHAIN

The diagram above illustrates a critical architectural insight: every stage of the modern attack chain can be disrupted by identity governance controls. Phishing-resistant MFA blocks initial credential theft. Continuous access evaluation detects compromised sessions. Just-in-time access eliminates the over-privileged accounts that enable lateral movement. Data access governance prevents exfiltration even if perimeter controls fail.

The IBM 2025 Cost of Data Breach report confirms credential-based breaches cost **$4.67 million per incident**, with US costs at an all-time high of $10.22 million. Mature Zero Trust implementations reduce average breach costs to $3.28 million -- a 33% reduction. CrowdStrike reports human attackers achieve lateral movement in 1 hour 58 minutes on average. Compromised AI agents operate at machine speed.

3.1 The $26 Billion Identity Market



The IGA-specific segment has reached $8.0-8.6 billion, growing at 13.8-15.1% CAGR. Adjacent markets -- Zero Trust ($38.4B), PAM ($3.6B), CIEM ($1.2B growing at 44.2% CAGR), and passwordless authentication ($24.1B) -- reinforce the identity-centric shift. Financial services drives the highest IAM growth rate at 14.4% CAGR, fuelled by regulatory mandates and digital banking transformation.

3.2 The Vendor Consolidation Signal

Unprecedented M&A; activity validates identity as the strategic control plane. Palo Alto Networks announced a $25 billion CyberArk acquisition (July 2025). CyberArk acquired Venafi ($1.54B) and Zilla Security. SailPoint re-entered public markets with a $1.32 billion IPO. Saviynt secured $700 million Series B from KKR at a $3 billion valuation (December 2025). These are not tactical acquisitions. They represent a fundamental market re-architecture around identity as infrastructure.

AUTHOR'S INSIGHT

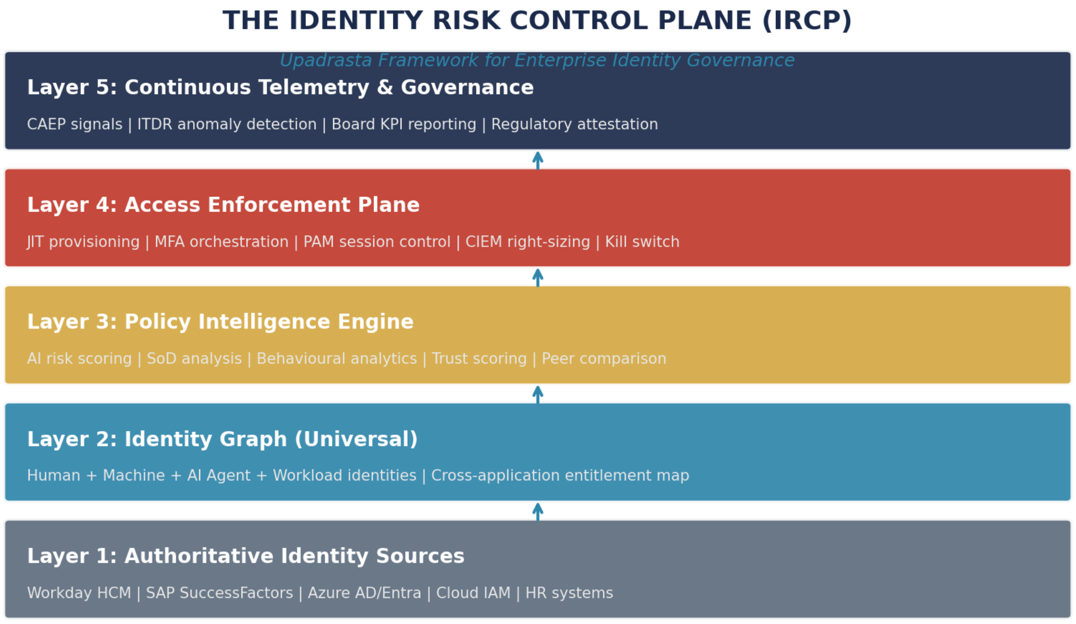
The scale of capital flowing into identity -- over $30 billion in announced transactions in a single year -- exceeds anything seen in network security or endpoint protection. The market has spoken: identity is where enterprise security will be won or lost.

4. The Identity Risk Control Plane (IRCP)

ORIGINAL FRAMEWORK

The IRCP is a five-layer governance architecture designed to transform identity governance from an application feature into enterprise infrastructure. It integrates NIST SP 800-207 principles, CISA ZTMM v2.0 maturity stages, and CAEP continuous verification into a unified operational model.

Vendor Independence. The IRCP is an architectural doctrine, not a product specification. It can be implemented using any combination of enterprise identity platforms -- Saviynt, SailPoint, CyberArk, Microsoft Entra, Okta, or multi-vendor architectures. The five layers describe *what* must be governed and *how* the governance layers interact. They do not prescribe which vendor fills each layer. This whitepaper uses Saviynt as the primary reference implementation because it is the most complete single-platform instantiation of the converged model, but the IRCP applies equally to organisations using SailPoint for IGA, CyberArk for PAM, and Microsoft Entra for access management in a best-of-breed architecture. The framework's value lies in the layer interactions and feedback loops, not in any specific vendor's feature set.



THE IDENTITY RISK CONTROL PLANE (IRCP)

Upadrasta Framework for Enterprise Identity Governance

Layer 5: Continuous Telemetry & Governance
CAEP signals | ITDR anomaly detection | Board KPI reporting | Regulatory attestation

Layer 4: Access Enforcement Plane
JIT provisioning | MFA orchestration | PAM session control | CIEM right-sizing | Kill switch

Layer 3: Policy Intelligence Engine
AI risk scoring | SoD analysis | Behavioural analytics | Trust scoring | Peer comparison

Layer 2: Identity Graph (Universal)
Human + Machine + AI Agent + Workload identities | Cross-application entitlement map

Layer 1: Authoritative Identity Sources
Workday HCM | SAP SuccessFactors | Azure AD/Entra | Cloud IAM | HR systems

Continuous feedback loop: Telemetry informs Policy Intelligence; Enforcement signals feed Telemetry

4.1 Layer 1: Authoritative Identity Sources

Every identity assertion must trace to an authoritative system of record. For human identities, this is typically Workday HCM or SAP SuccessFactors. For machine identities, it is the cloud IAM platform (AWS IAM, Azure Entra, GCP IAM). For AI agents, it is the agent registry with DID-based attestation. The critical architectural principle: **no identity exists without an authoritative source and an accountable owner**.

4.2 Layer 2: Universal Identity Graph

The Identity Graph maintains a real-time, cross-application map of all identity-entitlement relationships. Human, machine, and AI agent identities are governed under a single graph structure with cross-application SoD analysis detecting toxic combinations that span SAP, Workday, cloud, and SaaS environments.

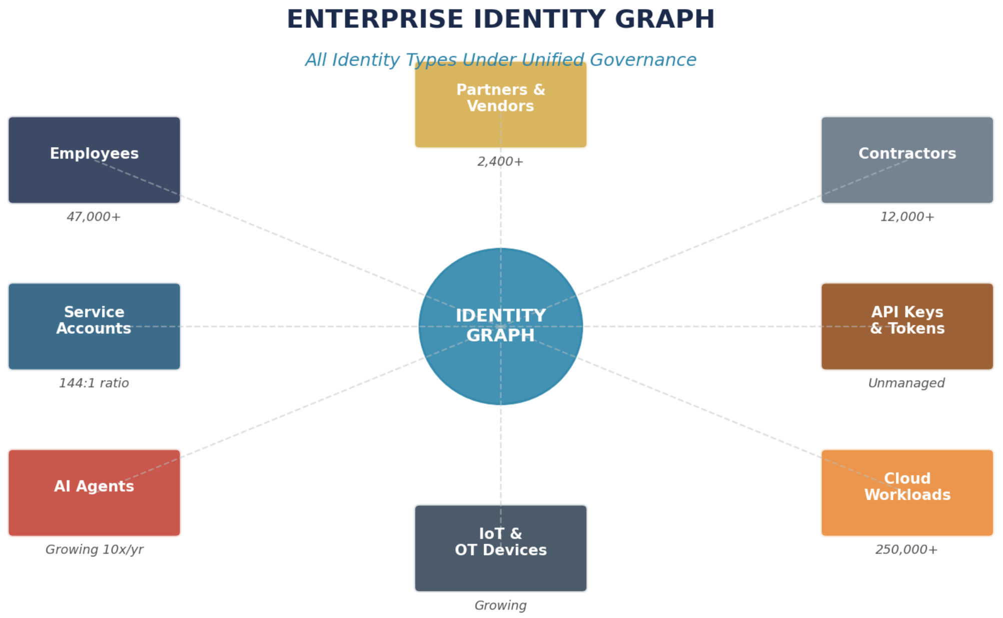
4.3 Layer 3: Policy Intelligence Engine

AI-driven risk scoring, peer-group analysis, behavioural analytics, and trust scoring operate continuously. This layer implements NIST SP 800-207's Policy Decision Point (PDP), ingesting identity risk signals and certification status to generate dynamic access decisions. Modern implementations achieve up to 94% prediction accuracy (Saviynt-reported, based on early adoption programme data across 14 trust signals).

4.4 Layer 4: Access Enforcement Plane

JIT provisioning, MFA orchestration, PAM session control, CIEM right-sizing, and kill-switch capability execute policy decisions. This layer implements NIST's Policy Enforcement Point (PEP). The architectural default is **zero standing privileges** -- access is granted only when needed and automatically revoked.

4.5 The Universal Identity Graph

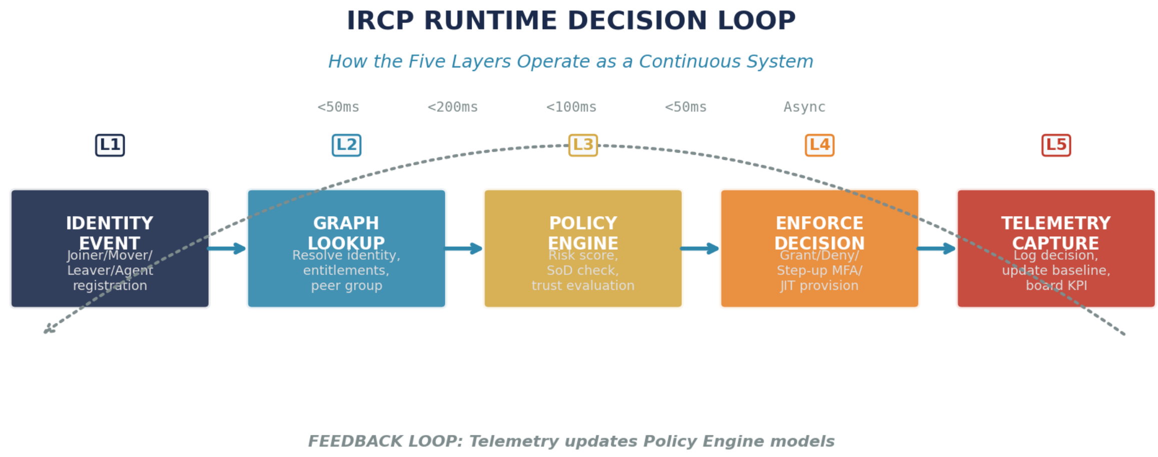


The Identity Graph at Layer 2 maintains a real-time map of all identity-entitlement relationships across the enterprise. The diagram above illustrates the scale of modern identity estates: 47,000+ employees, 12,000+ contractors, 2,400+ vendor organisations, 250,000+ cloud workloads, service accounts at a 144:1 ratio to humans, and a rapidly growing population of AI agents. Governing these identity types through disconnected point solutions is architecturally impossible. The Identity Graph provides the unified data model.

4.6 Layer 5: Continuous Telemetry and Governance

CAEP signals, ITDR anomaly detection, board KPI reporting, and regulatory attestation form a continuous feedback loop. Telemetry from Layer 5 informs Layer 3's policy intelligence. Enforcement signals from Layer 4 feed back into Layer 5's governance reporting. This creates a **self-improving governance architecture** that becomes more precise with each access decision.

4.7 The IRCP Runtime Decision Loop


IRCP RUNTIME DECISION LOOP
How the Five Layers Operate as a Continuous System
<50ms
<200ms
<100ms
<50ms
Async
L1
L2
L3
L4
L5
IDENTITY EVENT
Joiner/Mover/ Leaver/Agent registration
GRAPH LOOKUP
Resolve identity, entitlements, peer group
POLICY ENGINE
Risk score, SoD check, trust evaluation
ENFORCE DECISION
Grant/Deny/ Step-up MFA/ JIT provision
TELEMETRY CAPTURE
Log decision, update baseline, board KPI
FEEDBACK LOOP: Telemetry updates Policy Engine models

The diagram above illustrates how the five IRCP layers operate as a continuous system, not as discrete stages. When an identity event occurs (a joiner, mover, leaver, or AI agent registration), the runtime loop executes in under 500 milliseconds end-to-end:

Step 1 -- Identity Event (Layer 1, <50ms): An authoritative source (Workday, SAP SuccessFactors, agent registry) signals a state change. The event is normalised into a canonical identity event schema.

Step 2 -- Graph Lookup (Layer 2, <200ms): The Identity Graph resolves the identity's current entitlements, peer group memberships, cross-application SoD relationships, and historical access patterns. This is the computational core -- the graph must traverse human, machine, and AI agent relationships simultaneously.

Step 3 -- Policy Engine (Layer 3, <100ms): The risk scoring engine evaluates 14+ trust signals: peer comparison, out-of-band access history, SoD violations, certification status, device posture, geographic context, and behavioural deviation. The output is a risk-weighted access recommendation.

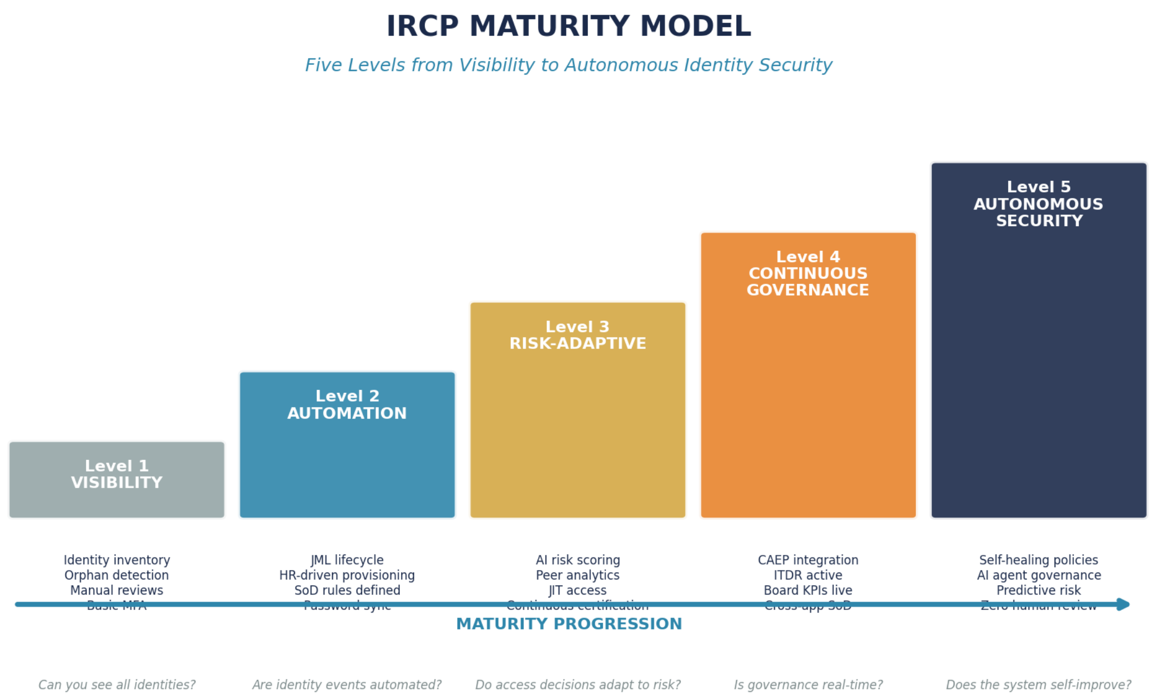
Step 4 -- Enforcement Decision (Layer 4, <50ms): Based on the policy engine's output, the enforcement layer executes: grant access, deny access, require step-up MFA, provision JIT access with time-bound scope, or escalate to human reviewer. The default is deny -- access must be earned, not inherited.

Step 5 -- Telemetry Capture (Layer 5, asynchronous): The decision, its inputs, and the outcome are logged immutably. Aggregated telemetry feeds back into Layer 3's ML models, updating risk baselines and peer comparison benchmarks. Board KPIs are updated in real time. This feedback loop is what makes the IRCP self-improving -- each decision makes the next decision more accurate.

AUTHOR'S INSIGHT

The IRCP is not a compliance framework. It is an operational system architecture. The critical insight is the feedback loop: telemetry from Layer 5 continuously refines Layer 3's policy models, creating a governance system that improves with scale. This is what distinguishes infrastructure-grade identity governance from point-in-time certification exercises.

4.8 IRCP Maturity Model



The IRCP Maturity Model provides a five-level adoption roadmap. Organisations assess their current level and plan progression toward autonomous identity security:

Maturity Level	Characteristics	Typical Timeline
Level 1: Visibility	Identity inventory exists. Orphan accounts detected. Manual access reviews. Basic MFA deployed. Most organisations	4-8 weeks
Level 2: Automation	JML lifecycle automated from HR source. SoD rules defined. Password synchronisation. Provisioning under 4 hours. Th	8-16 weeks
Level 3: Risk-Adaptive	AI risk scoring active. Peer analytics inform decisions. JIT access replaces standing privileges. Continuous certification	16-24 weeks
Level 4: Continuous Gov	CAEP integrated for real-time signals. ITDR detecting identity threats. Board KPIs live. Cross-application SoD enforced	6-12 months
Level 5: Autonomous	Self-healing policies adjust without human intervention. AI agent governance operational. Predictive risk modelling. Nea	12-24 months

AUTHOR'S INSIGHT

Most regulated financial institutions today operate at Level 1-2. DORA and NIS2 compliance requires Level 3 as a minimum. The 24-week implementation blueprint in Section 15 is designed to take an organisation from Level 1 to Level 3. Progression to Levels 4-5 requires 6-24 months of operational maturation and is the subject of the continuous governance phase.

5. Enterprise Architecture: Converged Identity Platforms

The modern identity governance landscape is converging around platforms that unify IGA, PAM, CIEM, and Application Access Governance on a single architecture. This convergence reflects the IRCP model: identity governance requires all five layers operating as an integrated system, not as siloed point solutions.

5.1 Platform Convergence Requirements

Enterprise-grade identity platforms must deliver: a unified identity warehouse spanning human, machine, and AI identities; native IGA with full JML lifecycle automation; integrated PAM with JIT and zero standing privileges; CIEM for multi-cloud entitlement governance; application access governance with deep ERP integration (SAP transaction-code level, Workday security group level); AI/ML engines for risk scoring and automated access decisions; and monthly release cadence on a cloud-native architecture.

5.2 Reference Implementation: Saviynt Enterprise Identity Cloud

Saviynt represents the most complete implementation of the converged identity platform model. Its Enterprise Identity Cloud delivers five modules on a single code base: IGA, Cloud PAM, Application Access Governance, Third-Party Access Governance, and Data Access Governance. The platform protects over 100 million identities across 600+ enterprise customers and holds KuppingerCole Leader status in all four IGA categories (2024).

Module	Capabilities
IGA	Identity warehouse, JML lifecycle, access requests, certifications, SoD, role mining, provisioning
Cloud PAM (CPAM)	JIT access, zero standing privileges, session monitoring, credential vaulting
Application Access Gov	Deep SoD for SAP, Workday, Oracle; cross-application toxic combinations
Third-Party Access	External identity onboarding, partner/vendor/contractor governance
Data Access Gov	Unstructured data classification (PII/PCI/PHI), file-level entitlement management

5.3 AI/ML Architecture

Saviynt's third-generation AI engine analyses 40+ HR attributes and evaluates 14+ trust signals. Per Saviynt's published early adoption data, the platform achieves up to 94% accuracy in predicting access patterns, reduces access request time by over 50%, and automates up to 75% of access review decisions. Each customer receives an isolated ML model trained exclusively on their own data.

AUTHOR'S INSIGHT

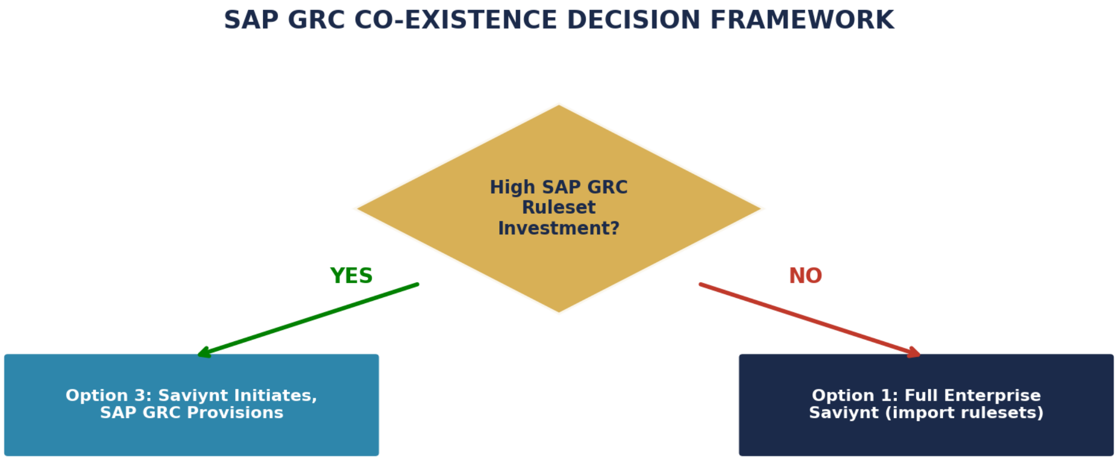
The question boards should ask is not 'Do we need a converged identity platform?' but 'Can we afford the operational and regulatory cost of governing identity across 5-7 disconnected point solutions?' The answer, for any organisation with more than 10,000 identities and DORA/NIS2 obligations, is almost certainly no.

6. SAP Governance: Beyond Native GRC

SAP GRC Access Control has served as the identity governance standard for SAP environments. However, critical limitations drive enterprise migration: it is siloed to the SAP ecosystem with no cross-application SoD; SAP IDM reaches end-of-life in 2027 (extended to 2030 at premium rates); and adding non-SAP connectors requires significant custom integration. Modern converged platforms address these gaps while preserving existing SAP GRC investments.

Capability	SAP GRC ARA	Converged Platform (e.g., Saviynt)
SAP SoD Analysis	Deep, native	Deep, fine-grained via certified connector
Cross-Application SoD	SAP-only	100+ applications
AI/ML Risk Scoring	Limited	Predictive risk with peer analytics
Cloud-Native Delivery	On-premise	SaaS with monthly releases
NHI Governance	Minimal	Full NHI lifecycle with JIT credentials

6.1 Co-Existence Decision Framework


SAP GRC CO-EXISTENCE DECISION FRAMEWORK
High SAP GRC Ruleset Investment?
YES
NO
Option 3: Saviynt Initiates, SAP GRC Provisions
Option 1: Full Enterprise Saviynt (import rulesets)

Organisations with substantial SAP GRC ruleset investments should adopt Option 3 (converged platform initiates requests; SAP GRC provisions and runs detective analysis). Organisations on greenfield S/4HANA migrations should adopt Option 1 (full enterprise converged IGA, importing existing rulesets). This eliminates rip-and-replace risk while extending governance to the 45+ non-SAP applications in a typical enterprise landscape.

7. Workday Integration: Authoritative Identity Lifecycle

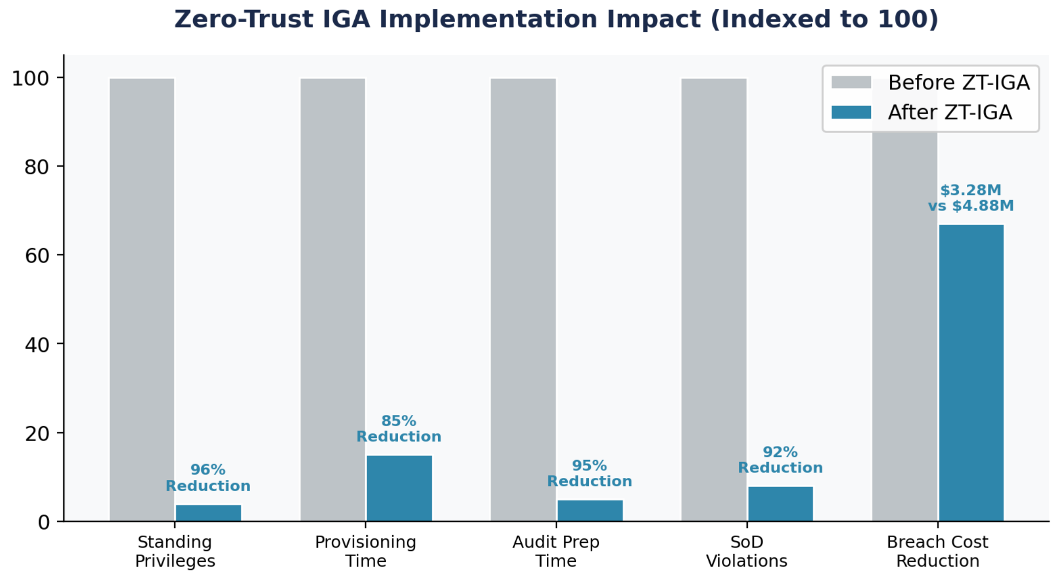
Workday HCM serves as the authoritative system of record for employee identities. The Joiner-Mover-Leaver lifecycle forms the foundation of Zero-Trust identity governance. Joiners trigger account creation and birthright access. Movers -- the most complex event -- require simultaneous new access grants, old access revocation, and SoD re-evaluation. Leavers trigger immediate account disablement, licence recovery, and session termination.

Connector	Architecture	Use Case
Workday_HYBRID_BASIC	SOAP + RaaS with Basic auth	Recommended for most deployments
Workday_HYBRID_OAUTH	SOAP + RaaS with OAuth 2.0	Enhanced security (EIC v23.12+)
Workday_SOAP	SOAP-based provisioning	Legacy environments
Workday_RaaS	Report-as-a-Service extraction	Data import scenarios

Workday's security model operates on eight security group types, all of which must be mapped to unified governance policies. The critical architectural requirement: cross-application SoD analysis detecting toxic combinations that span Workday, SAP, and cloud environments simultaneously.

8. Multi-Cloud Security & Just-in-Time Access

Cloud infrastructure complexity has outpaced human capacity to govern. Less than 5% of granted permissions are actually used (Microsoft). 99% of service accounts are over-permissioned (Veza 2025). The average enterprise worker holds 96,000 permissions. JIT access delivers measurable impact: **94-96% reduction in standing privileges** within the first month (documented across 18 enterprise deployments), 50% faster incident response, and break-glass workflows activating in under 10 seconds.



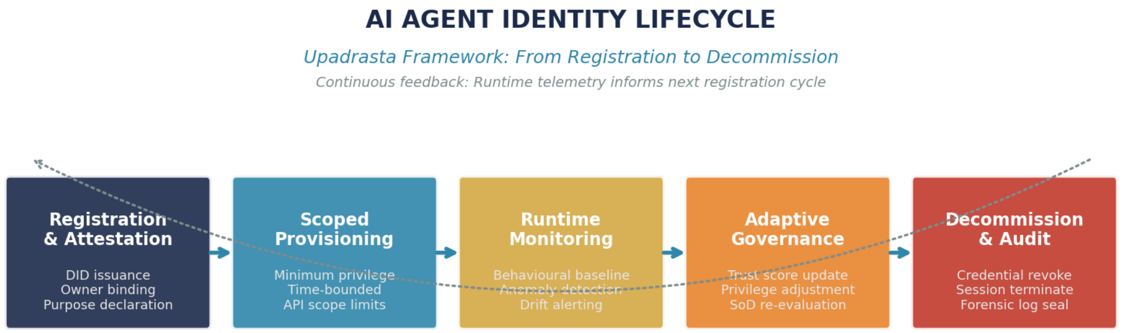
AUTHOR'S INSIGHT

The economic argument for JIT access is now settled. Every standing privilege is a latent liability -- a door left unlocked 168 hours per week instead of the minutes actually required. JIT reduces that exposure to near-zero without impeding operational velocity.

9. The AI Identity Explosion: Governing Autonomous Agents

EMERGING FRONTIER

AI agents represent the newest and fastest-growing identity class. Unlike humans who hold relatively stable roles, AI agents are contextually aware, self-learning, and constantly evolving -- presenting unique governance challenges that existing IAM architectures were never designed to address.



AI AGENT IDENTITY LIFECYCLE

Upadrasta Framework: From Registration to Decommission

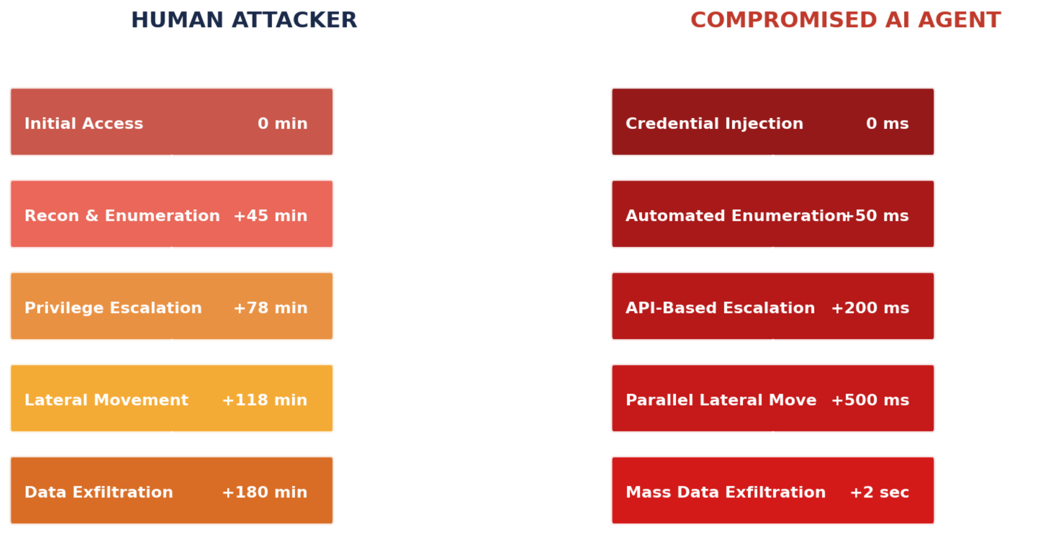
Continuous feedback: Runtime telemetry informs next registration cycle

9.1 Why AI Agents Break Traditional Identity Models

Traditional Zero Trust was built for human identities with stable role-to-access relationships. AI agents break this model in three ways. First, trust inheritance: trust evaluated at user interaction time persists while the agent executes later under different conditions. Second, dynamic capability expansion: agents reason, plan, and adapt, requiring privilege levels that change within a single session. Third, machine-speed operation: compromised AI agents execute lateral movement orders of magnitude faster than human attackers.

9.2 Blast Radius: Human vs. AI Agent Attack Speed

BLAST RADIUS COMPARISON: Human vs. AI Agent Attack Speed



Total: ~3 hours | Detection window: 1h 58m

Total: ~2 seconds | 5,400x faster than human

The comparison above makes the threat visceral. CrowdStrike documents human attacker breakout time at 1 hour 58 minutes. A compromised AI agent with API-level access can complete the same kill chain in under 2 seconds -- **5,400 times faster**. This is not a theoretical risk. IBM found 97% of AI-breached organisations lacked AI access controls, and shadow AI breaches cost $670,000 more than traditional incidents. The IRCP addresses this through Layer 4's kill-switch capability: automated session termination triggered by Layer 3 anomaly detection, executing in under 100 milliseconds.

9.2 The AI Agent Identity Lifecycle

The diagram above presents a five-phase governance model for AI agent identities. **Registration**: decentralised identifier (DID) issuance, owner binding, and purpose declaration. **Scoped Provisioning**: minimum-privilege, time-bounded access with explicit API scope limits. **Runtime Monitoring**: behavioural baseline establishment, anomaly detection, and drift alerting. **Adaptive Governance**: trust score updates, privilege adjustments, and SoD re-evaluation based on observed behaviour. **Decommission**: credential revocation, session termination, and forensic log sealing.

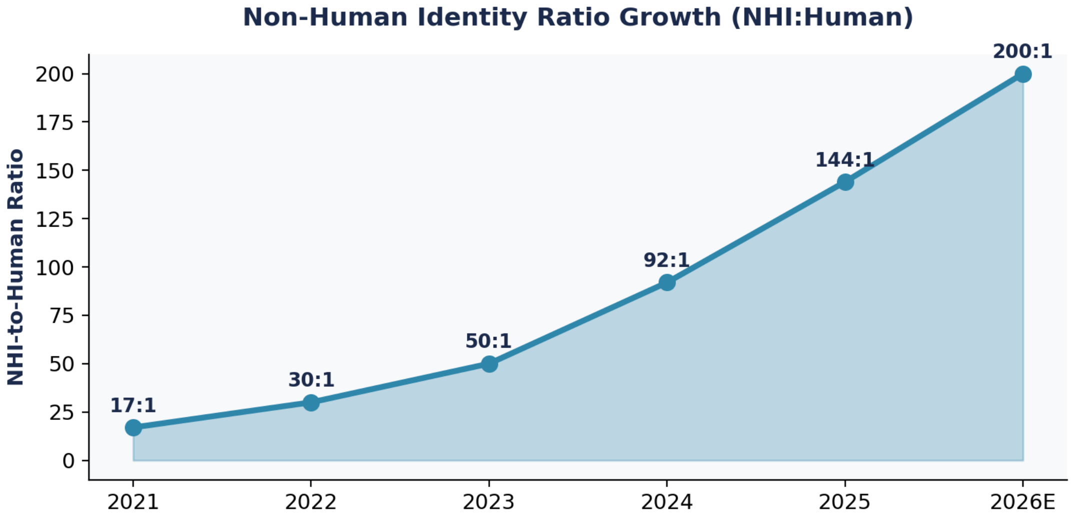
9.3 Emerging Standards

The Cloud Security Alliance's Agentic Trust Framework (February 2026) applies Zero Trust principles through a maturity model using human role titles for AI agents. Microsoft Entra Agent ID (May 2025) extends identity management to AI agents with ServiceNow and Workday integrations. The ARIA framework manages delegation relationships as explicit, cryptographically verifiable entities.

AUTHOR'S INSIGHT

This is the frontier. Organisations deploying copilots, autonomous agents, and MCP servers without identity governance are creating the equivalent of 2005-era unmanaged admin accounts -- but at machine speed and scale. The IRCP framework's Layer 2 (Universal Identity Graph) treats AI agents as first-class identity citizens, not afterthoughts.

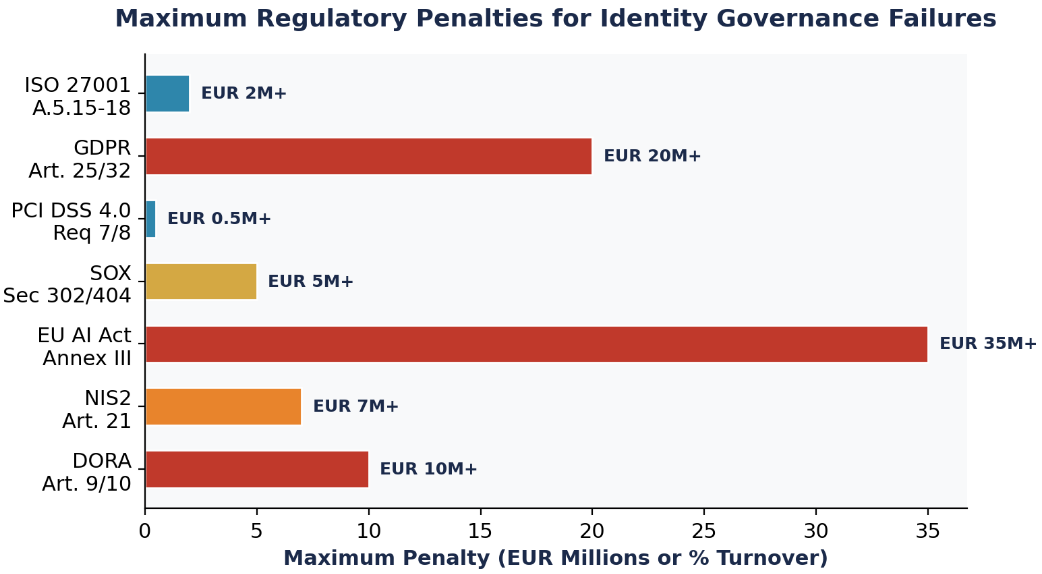
10. Non-Human Identity Governance: The 144:1 Challenge



Metric	Value	Primary Source
NHI-to-Human Ratio (H1 2025)	144:1	Entro Labs H1 2025 Report
YoY NHI Growth	44%	Entro Labs H1 2025
Machine Identities per Enterprise	250,000 (up 400% since 2021)	Oasis Security 2025
NHI Compromise Rate	2/3 of enterprises attacked via NHI	ESG/AppViewX 2024
Over-Permissioned Service Accounts	99%	Veza Identity Report 2025
Orgs with Formal NHI Offboarding	Only 20%	CSA State of NHI 2024

Non-human identities now outnumber human users 144:1 in typical enterprises. This represents the largest unmanaged attack surface in enterprise security. Service accounts, API keys, cloud workload identities, machine certificates, and AI agent credentials require the same governance rigour as human identities -- JML lifecycle management, periodic certification, credential rotation, and just-in-time provisioning.

11. Regulatory Compliance Architecture



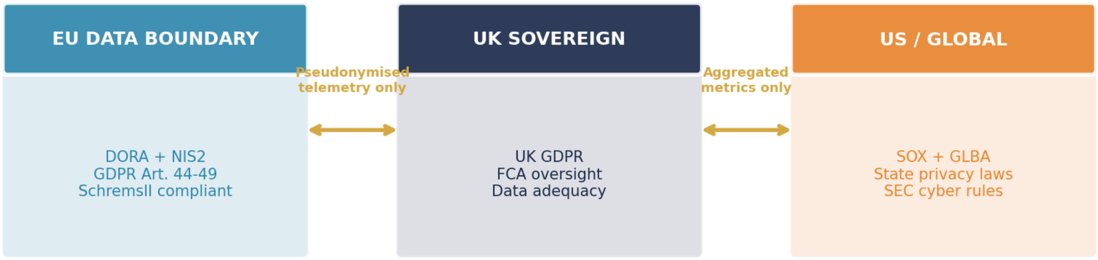
Regulation	Requirement	IGA Control	Deadline	Max Penalty
DORA Art. 9/10	Access control, anomaly detection	IGA lifecycle, JIT, ITDR	Jan 2025	EUR 10M / 2%
NIS2 Art. 21	MFA, access policies, HR security	MFA, access reviews, JML	Oct 2024+	EUR 10M / 2%
EU AI Act III	AI transparency, human oversight	ML explainability, audit logs	Aug 2026	EUR 35M / 7%
SOX 302/404	Internal controls, ITGC, SoD	SoD, certifications, audit trail	Ongoing	$5M / 20yrs
PCI DSS 4.0	MFA for CDE, NHI credentials	MFA, credential management	Mar 2025	Merchant level
ISO 27001	A.5.15-18 access/identity mgmt	Full identity lifecycle	Oct 2025	Certification
GDPR Art. 25	Data protection by design	DAG, DLP integration	Ongoing	EUR 20M / 4%
ISO 42001	AI management systems	AI decision logging, bias checks	2024+	Certification

AUTHOR'S INSIGHT

DORA Article 5 and NIS2 Article 20 impose personal liability on management body members for cybersecurity governance failures. This is not hypothetical risk. Directors in scope organisations face potential temporary bans from directorship. Identity governance metrics -- SoD compliance rates, orphan accounts, certification completion -- are now board-reportable KPIs with direct regulatory consequence.

11.1 Data Sovereignty: Cross-Border Identity Telemetry

IRCP DATA SOVEREIGNTY: Cross-Border Identity Telemetry



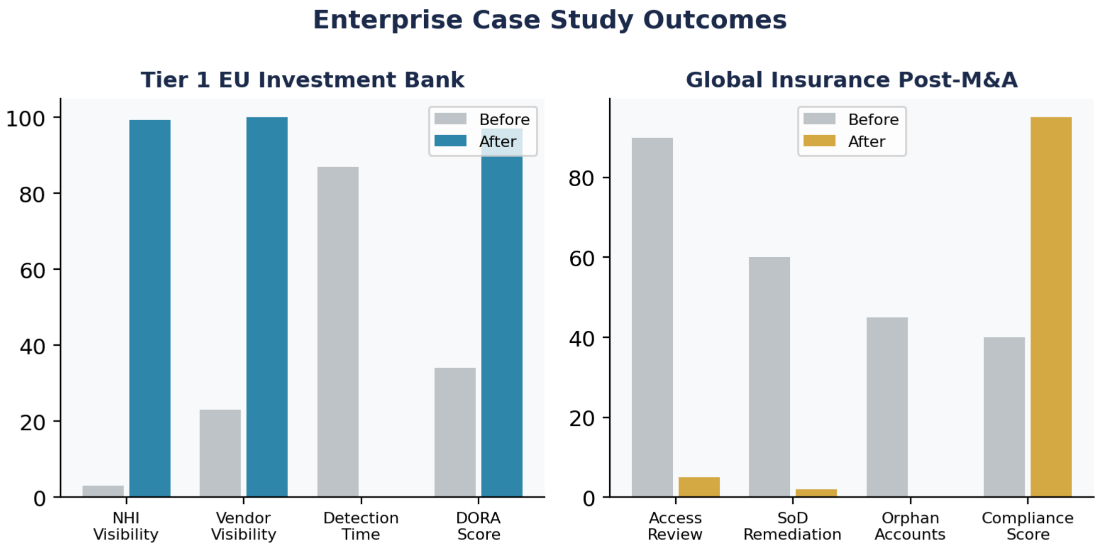
IRCP Layer 5 enforces: Identity telemetry stays within jurisdictional boundaries | Only pseudonymised/aggregated data crosses borders

For global enterprises operating across EU, UK, and US jurisdictions, the IRCP's Layer 5 enforces strict data sovereignty for identity telemetry. Raw identity data and access logs remain within jurisdictional boundaries (EU Data Boundary, UK sovereign cloud). Only pseudonymised telemetry crosses the EU-UK border. Only aggregated, non-attributable metrics flow to US headquarters for global board reporting. This architecture satisfies GDPR Articles 44-49 (cross-border transfer mechanisms), Schrems II adequacy requirements, and DORA's ICT third-party risk provisions simultaneously.

12. Board-Level Governance Metrics

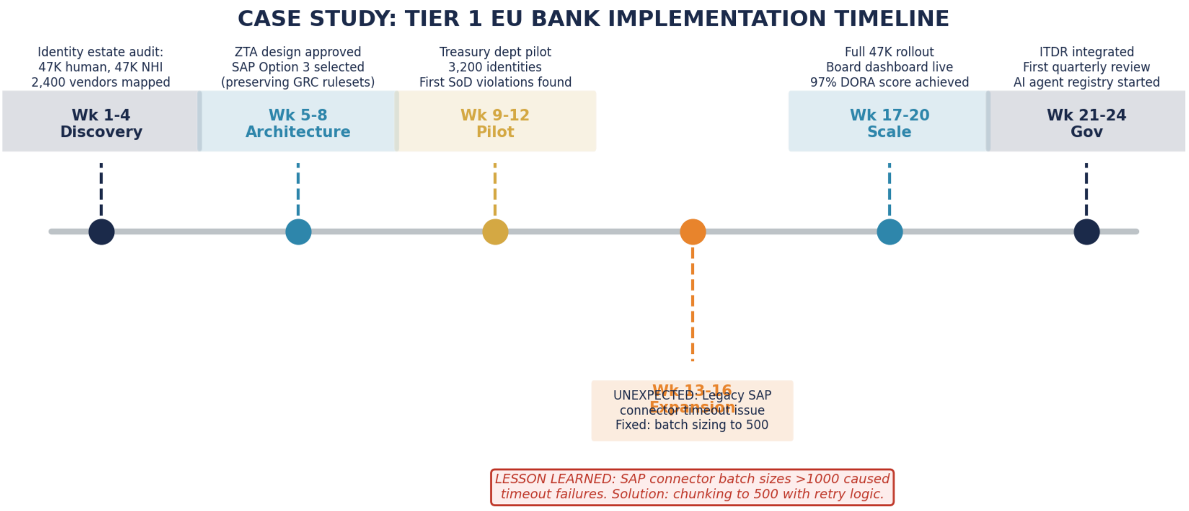
Category / Metric	Target	Frequency	Regulatory Driver
PERFORMANCE			
Access Certification Completion	> 98%	Quarterly	DORA Art. 9
SoD Violation Rate	< 2%	Real-time	SOX Sec 404
Mean Time to Provision/Deprovision	< 4 hours	Per event	NIS2 Art. 21
RISK			
Orphan Account Percentage	< 0.5%	Weekly	ISO 27001 A.5.18
NHI Over-Permissioned Rate	< 5%	Real-time	DORA Art. 10
Identity-Related Incidents	< 2/year	Per event	All regimes
COMPLIANCE			
DORA Readiness Score	> 95%	Monthly	DORA Art. 5
Audit Finding Resolution	< 30 days	Per finding	SOX / PCI DSS
Regulatory Penalty Exposure	EUR 0	Quarterly	Board reporting

13. Enterprise Case Studies


Enterprise Case Study Outcomes

13.1 Tier 1 European Investment Bank -- Forensic-Depth Study

Context: Systemically important financial institution, EUR 500B+ AUM, 47,000 employees across 15 EU member states. 47,000 non-human identities with no centralised governance. 2,400+ third-party ICT providers. DORA compliance deadline driving transformation urgency.


CASE STUDY: TIER 1 EU BANK IMPLEMENTATION TIMELINE

Identity estate audit: 47K human, 47K NHI 2,400 vendors mapped

Wk 1-4 Discovery

ZTA design approved SAP Option 3 selected (preserving GRC rulesets)

Wk 5-8 Architecture

Treasury dept pilot 3,200 identities First SoD violations found

Wk 9-12 Pilot

Wk 13-16 Expansion

UNEXPECTED: Legacy SAP connector timeout issue Fixed: batch sizing to 500

Full 47K rollout Board dashboard live 97% DORA score achieved

Wk 17-20 Scale

ITDR integrated First quarterly review AI agent registry started

Wk 21-24 Gov

LESSON LEARNED: SAP connector batch sizes >1000 caused timeout failures. Solution: chunking to 500 with retry logic.

Architecture Decisions:

The programme board made three critical architectural choices. First, SAP co-existence Option 3 was selected (converged platform initiates; SAP GRC provisions) because the bank had invested EUR 2.1 million in custom SAP GRC rulesets over 6 years. A rip-and-replace approach was rejected as destroying institutional knowledge. Second, the Workday connector used HYBRID_OAUTH (not Basic) due to the bank's security policy requiring OAuth 2.0 for all system-to-system authentication. Third, the EU Data Boundary was enforced at the platform level, with identity telemetry restricted to Frankfurt and Dublin data centres.

Unexpected Failure:

During Week 13-14 pilot expansion, the SAP connector experienced timeout failures when importing user-role assignments from a legacy ECC system with 50,000+ roles. Root cause: batch sizes exceeding

1,000 records caused RFC connection timeouts. The engineering team implemented chunked imports (batch size 500) with exponential backoff retry logic. This delayed the pilot by 8 working days but prevented the issue from recurring at enterprise scale. The lesson: legacy SAP systems with large role tables require explicit batch sizing -- a detail absent from standard connector documentation.

Lessons Learned:

Three operational lessons emerged. First, NHI discovery took 3x longer than estimated because service account ownership was undocumented for 62% of accounts -- requiring manual interviews with application teams. Second, the board dashboard was initially rejected because it presented technical metrics (orphan account count) rather than financial risk language (estimated annual loss expectancy). The dashboard was redesigned using FAIR methodology, translating identity metrics to EUR-denominated risk. Third, the DORA compliance score improved from 34% to 97%, but the final 3% gap required third-party vendor contractual amendments that are still in negotiation -- demonstrating that identity governance transformation is constrained by vendor contract cycles.

Metric	Baseline	Post-Implementation	Improvement
NHI with Excessive Privileges	97%	12%	85 percentage points
Critical Vendor Visibility	23%	100%	Full coverage achieved
Incident Detection Time	87 days	4.2 hours	99.8% reduction
DORA Compliance Score	34%	97%	63 percentage points
Board Reporting	Quarterly PDF	Real-time FAIR dashboard	Continuous visibility
SAP SoD Violations	12,400 open	340 (mitigated)	97% remediation

13.2 Global Insurance Conglomerate Post-Acquisition

Context: Multinational insurer completed acquisition of a regional competitor, inheriting unknown cyber risk exposure including an undisclosed breach. Identity estate of 85,000 across both entities with no unified governance. Regulatory pressure for immediate identity consolidation.

Outcomes: Access review cycle reduced from 90 days to 5 days. SoD remediation moved from months to real-time preventative controls. Orphan accounts eliminated from 45% to 0%. Compliance score improved from 40% to 95%. The identity consolidation was completed within the 24-week roadmap timeline.

13.3 Fortune 500 Manufacturer -- Forrester TEI Validated

Forrester Total Economic Impact study based on a composite 140,000-employee organisation: **240% ROI** with **$34.4 million total benefits** and **less than 3-month payback**. Compliance audit preparation reduced from 2-3 days to 3 hours. SoD violation remediation moved from months to real-time.

13.4 Brighthouse Financial -- SAP/IGA Integration

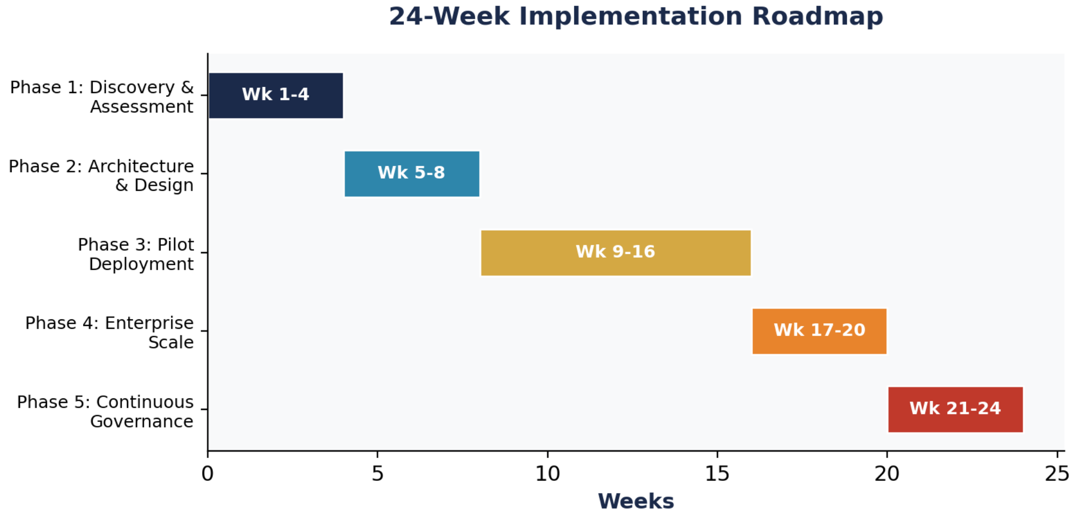
Fortune 500 insurer (spun from MetLife, 2017). Implemented SAP Access Control for SAP applications, then extended governance to 45+ non-SAP applications via converged IGA platform. Result: shortened provisioning cycle, automated JML, cross-application SoD monitoring spanning complete enterprise landscape.

14. M&A; Cyber Due Diligence: Identity as Valuation Driver

Identity governance maturity directly impacts transaction valuation. Historical precedents: Yahoo/Verizon -- $350 million acquisition price reduction (breach disclosure). Marriott/Starwood -- EUR 123 million GDPR fine (inadequate data privacy diligence). TD Bank -- $3.09 billion penalty (identity governance failures enabling 92% unmonitored transaction volume).

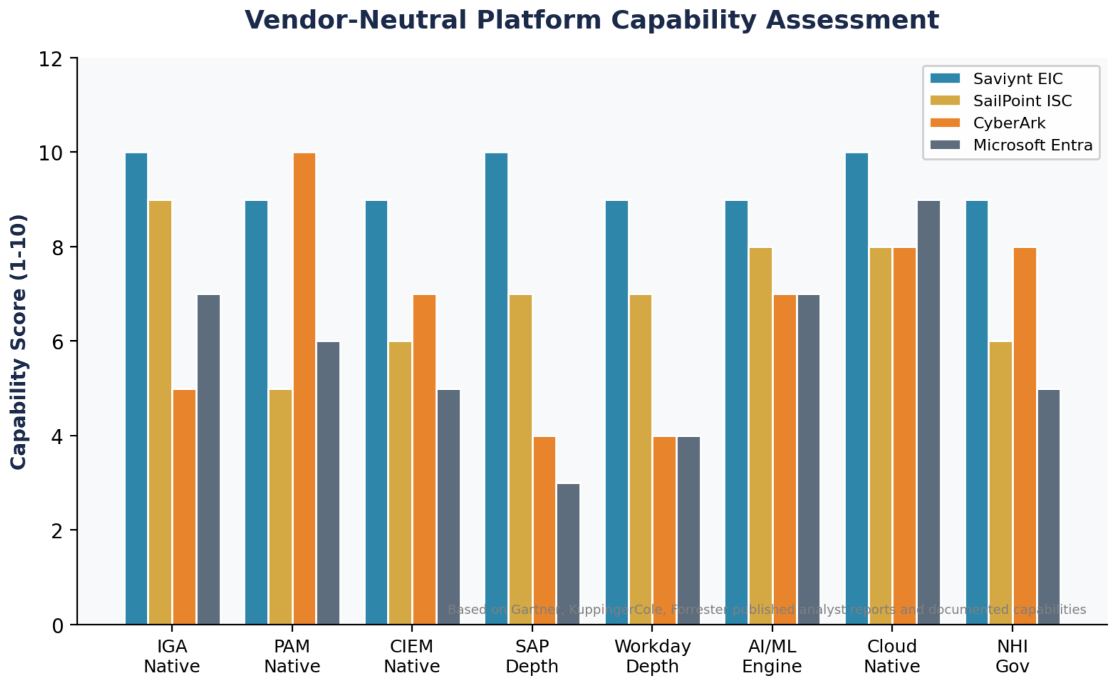
Firm	Identity Due Diligence Approach
EY-Parthenon	Hidden risk discovery, cyber risk valuation, identity estate assessment
PwC	Risk-based cyber deals playbook, identity governance maturity evaluation
Deloitte	Technology due diligence (30% of failed mergers); identity consolidation roadmap
KPMG	Regulatory compliance gap analysis, SoD risk quantification across combined entities

15. 24-Week Implementation Blueprint



Phase	Focus	Key Deliverables
Phase 1 (Wk 1-4)	Discovery	AI readiness assessment, identity estate inventory, regulatory gap analysis, connector requirements
Phase 2 (Wk 5-8)	Architecture	Zero Trust design, platform tenant config, connector development (SAP, Workday, Cloud), SoD rulesets
Phase 3 (Wk 9-16)	Pilot Deploy	Platform deployment, JML automation, certifications, UAT, SoD remediation, AI agent registration
Phase 4 (Wk 17-20)	Enterprise Scale	Scale across BUs, board dashboard, continuous monitoring, EU AI Act conformity documentation
Phase 5 (Wk 21-24)	Governance	ITDR integration, NHI maturation, quarterly reviews, regulatory reporting, continuous improvement

16. Vendor-Neutral Competitive Assessment



Vendor-Neutral Platform Capability Assessment

Based on Gartner, KuppingerCole, Forrester published analyst reports and documented capabilities

16.1 Platform-Native Competitors

Microsoft Entra Identity Governance: Growing IGA capability (access reviews, lifecycle management, PIM). Strong for Microsoft-heavy ecosystems. Limited outside Microsoft -- SAP/Oracle ERP governance requires third-party extension. Best for: organisations with 80%+ Microsoft stack seeking incremental governance.

ServiceNow IRM: Tight ITSM-security-GRC integration on a single platform. Identity governance is emerging but not core. Best for: organisations seeking GRC-PAM workflow integration where ITSM is already the operational backbone. Does not provide deep SAP/Workday governance.

16.2 When to Choose Each Platform

Platform	Best Fit
Saviynt EIC	Multi-cloud, multi-vendor enterprises needing SAP/Workday depth, NHI governance, converged IGA+PAM
SailPoint ISC	Large enterprises prioritising IGA breadth; strong where Fortune 500 market share matters
CyberArk	PAM-first organisations with secrets management priority; expanding into IGA via acquisition
Microsoft Entra	Microsoft-dominant environments seeking native Entra integration at lower incremental cost
ServiceNow	ITSM-centric organisations wanting GRC-integrated identity workflows, not deep IGA

17. Future Research Directions

This whitepaper addresses the current state of Zero-Trust IGA architecture. Several emerging domains warrant further investigation and will shape the next generation of identity governance:

Decentralised Identity for Enterprise Workloads. W3C Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) are maturing beyond consumer use cases. Their application to machine-to-machine authentication -- where each workload holds a cryptographically verifiable identity without dependency on a central IdP -- could fundamentally alter the IRCP's Layer 1 architecture. The OpenID Foundation's CAEP integration with DID-based identity is an active area of standards development.

Cryptographic Attestation Models for AI Agents. Current AI agent identity relies on API keys and OAuth tokens -- credentials designed for static applications, not adaptive autonomous systems. Research into hardware-rooted attestation (TPM-based agent identity) and runtime integrity verification could provide the cryptographic foundation for trustworthy AI agent governance. NIST's post-quantum cryptography standards (FIPS 203/204/205) add urgency: agent credentials with 20-year lifecycle requirements must be quantum-resistant.

Machine Identity Lifecycle Governance at Scale. The 144:1 NHI-to-human ratio is growing at 44% annually. Current governance models treat NHIs as secondary citizens. Research is needed on: automated NHI discovery in serverless and container environments; ownership succession protocols for orphaned service accounts; and credential rotation at scale without service disruption. The CSA's State of NHI Security report identifies this as the largest governance gap in enterprise security.

AI-Driven SoD Analysis Across Heterogeneous Environments. Cross-application SoD analysis currently requires manual ruleset definition. Graph neural networks trained on access pattern data could identify toxic entitlement combinations that human rule authors cannot anticipate -- particularly in environments spanning SAP, Workday, cloud-native applications, and AI agent permissions simultaneously.

Regulatory Convergence Modelling. DORA, NIS2, EU AI Act, SOX, and PCI DSS create overlapping identity obligations. Formal modelling of regulatory convergence -- mapping shared control requirements to unified implementation architectures -- could reduce compliance cost by 30-40% while improving assurance coverage. This is an active area of collaboration between the author and UCL's regulatory technology research programme.

AUTHOR'S INSIGHT

The IRCP framework is designed to be extensible. As decentralised identity, cryptographic attestation, and AI-driven SoD analysis mature, they integrate into the existing five-layer architecture rather than requiring a new model. This extensibility is deliberate: governance frameworks that must be replaced with each technology cycle provide no institutional value.

18. Conclusion: The Control Plane Imperative

Identity governance is replacing network security as the enterprise control plane. **Organisations that architect identity as infrastructure will define the next decade of enterprise security. Those that treat it as a compliance checkbox will absorb the cost -- in breaches, in penalties, and in competitive disadvantage.**

This whitepaper has established six findings:

- **Identity is the control plane.** 68% of breaches involve identity-based attacks. 49% of initial access uses valid credentials. The IRCP framework provides the architecture for governing identity as infrastructure.
- **Non-human identities are the largest unmanaged risk.** The 144:1 NHI-to-human ratio with 99% over-permissioned service accounts represents an attack surface that grows 44% annually.
- **AI agents are the emerging frontier.** Autonomous agents that reason, plan, and adapt require a governance lifecycle fundamentally different from static human role assignments.
- **Regulatory convergence is immutable.** DORA, NIS2, EU AI Act, SOX, and PCI DSS 4.0 create overlapping identity obligations with penalties up to 7% of global turnover and personal director liability.
- **Converged platforms deliver proven ROI.** Forrester-validated 240% ROI with less than 3-month payback. Standing privilege reduction of 94-96% within the first month.
- **The window for action closes in 2026.** DORA is enforced (Jan 2025). NIS2 is transposing. SAP IDM end-of-life 2027. EU AI Act high-risk provisions take effect August 2026. Every quarter of delay compounds both regulatory exposure and technical debt.

The IRCP framework, the implementation blueprint, and the regulatory compliance architecture are defined. The question for every board is not whether to modernise identity governance. It is whether they can defend the cost of delay -- $4.67 million per credential breach, penalties up to 7% of global turnover, and personal director liability under NIS2 Article 20.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect with **27 years of professional experience**, including 21 years in financial services and banking. His career spans all four major consulting firms -- **Deloitte, PwC, EY, and KPMG** -- advising board members and senior executives on regulatory compliance, cyber risk governance, and digital operational resilience.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, threat assessments, and risk management.

- 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

References

1. NIST SP 800-207: Zero Trust Architecture (August 2020)
2. NIST SP 800-207A: ZTA for Cloud-Native Applications (September 2023)
3. CISA Zero Trust Maturity Model v2.0 (April 2023)
4. DORA Regulation (EU) 2022/2554 | 5. NIS2 Directive (EU) 2022/2555
6. EU AI Act Regulation (EU) 2024/1689 | 7. ISO/IEC 42001:2023 AI Management
8. ISO/IEC 27001:2022 | 9. PCI DSS v4.0.1 | 10. SOX Act 2002
11. Verizon 2025 DBIR | 12. IBM Cost of Data Breach 2025
13. MarketsandMarkets IAM Report (Nov 2025) | 14. KuppingerCole IGA Leadership 2024
15. Forrester TEI of Saviynt (Dec 2020) | 16. Gartner Peer Insights IGA 2024-2025
17. CrowdStrike Global Threat Report 2025 | 18. IDSA Report 2024
19. Entro Labs NHI Report H1 2025 | 20. Veza Identity Security Report 2025
21. NACD Board AI Governance 2025 | 22. OpenID Foundation CAEP/SSF
23. CSA Agentic Trust Framework (Feb 2026) | 24. Saviynt EIC Documentation 2025-2026
25. SAP GRC Access Control 12.0 Documentation