WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Identity-First Security Architecture

Modern Identity Governance — Lifecycle, Privileged Access, Federation & Machine Identity Control Plane

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years Cyber Security Experience | 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

Primary Audience: IAM Programme Leads / Identity Architects | Unique Artifact: Identity Risk Taxonomy & Control Plane Architecture

April 2026 | Cyber AI Systems Inc. | www.kie.ie

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

Table of Contents

1. Executive Dashboard

100%	Zero	< 5 min	Real-time
Identity Visibility	Standing Privilege	Access Provisioning	Risk Scoring

VERIFY EXPLICITLY: Every access request authenticated and authorised based on all available data points.

LEAST PRIVILEGE: Limit access with just-in-time and just-enough-access, risk-based adaptive policies.

ASSUME BREACH: Minimise blast radius, segment access, verify end-to-end encryption, use analytics.

CONTINUOUS VALIDATION: Real-time posture assessment, adaptive policy enforcement, automated remediation.

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

FLAGSHIP DOCTRINE STATEMENT: Identity Risk = f(entitlement_scope, activity_recency, owner_status, privilege_level). Kill-switch activates when any NHI exceeds baseline behavioural invariants.

2. Reference Architecture — Control Chain

The architecture below is structured as a control chain. Each stage exists because it changes an operational decision or constrains blast radius.

Identity Discovery	Lifecycle Governance	Privileged Access	Federation Trust	Machine Identity Control	Risk Scoring
Input	*Control Gate*	*Control Gate*	*Control Gate*	*Control Gate*	*Evidence / Output*

Deterministic Decision Engine

Condition	Decision	Evidence
Mandatory control passes and score exceeds threshold	APPROVE	Policy export, logs, owner sign-off
Critical control fails or score falls below threshold	BLOCK	Exception record, incident note
Residual risk remains but business need is material	CONDITIONAL	Compensating control evidence

2. Technical Abstract

Identity governance in the modern enterprise extends far beyond human user provisioning. Machine identities, service accounts, workload identities, and agentic AI systems now outnumber human identities by an order of magnitude — yet most organisations lack lifecycle governance for these non-human principals. This paper presents the Identity Control Plane Architecture with comprehensive lifecycle governance: joiner-mover-leaver models for both human and machine identities, PAM integration patterns, federation trust frameworks, an NHI lifecycle dashboard with kill-switch protocols, and an identity risk taxonomy that enables risk-based access decisions. The framework includes risk scoring formulas and machine-identity failure case analysis.

Primary Audience: IAM Programme Leads / Identity Architects
Unique Artifact: Identity Risk Taxonomy & Control Plane Architecture

Key Enhancements in This Edition:

- Lifecycle governance: JML model
- PAM integration patterns
- Machine identity governance framework
- NHI Lifecycle table with kill-switch status
- Identity risk taxonomy distinct from WP01/WP13

3. Problem: Identity as the Primary Attack Surface

The identity attack surface has expanded beyond human user accounts. Forrester Research estimates that non-human identities (service accounts, managed identities, API keys, workload identities) outnumber human identities by ratios of 10:1 to 45:1 in large enterprises. Yet most organisations lack lifecycle governance for these machine principals: no joiner-mover-leaver process, no entitlement review, no deprovisioning automation, no risk scoring.

The risk is concrete: a dormant service account with elevated privileges becomes an attacker's persistence mechanism. An API key with broad permissions embedded in a CI/CD pipeline becomes a supply-chain attack vector. This paper addresses the full identity lifecycle for both human and machine identities through the Identity Control Plane Architecture.

THREAT MODEL: Dormant service accounts used for persistence | API key theft from CI/CD pipelines | Machine identity privilege escalation through managed identity abuse | Federation trust exploitation through compromised identity providers | NHI entitlement sprawl creating excessive access paths.

5. Lifecycle Governance: Joiner-Mover-Leaver

This paper introduces the following contributions specific to identity-first security architecture. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Lifecycle governance: JML model
- PAM integration patterns
- Machine identity governance framework
- NHI Lifecycle table with kill-switch status
- Identity risk taxonomy distinct from WP01/WP13

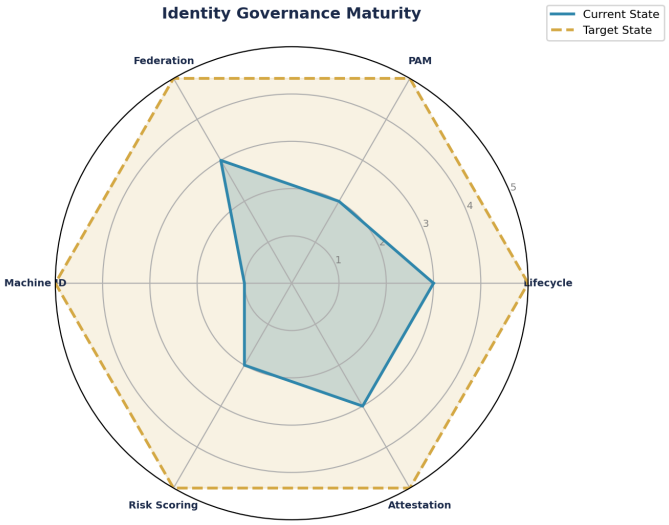

Figure 1: Identity Risk Taxonomy & Control Plane Architecture — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Identity governance obligations span DORA (ICT third-party and access management), NIS2 (identity as a risk management measure), ISO 27001:2022 Annex A.5.15-5.18 (access control), and the emerging NHI governance requirements under the EU AI Act for machine identities. The Identity Control Plane Architecture addresses these obligations through a unified lifecycle model for human and machine identities.

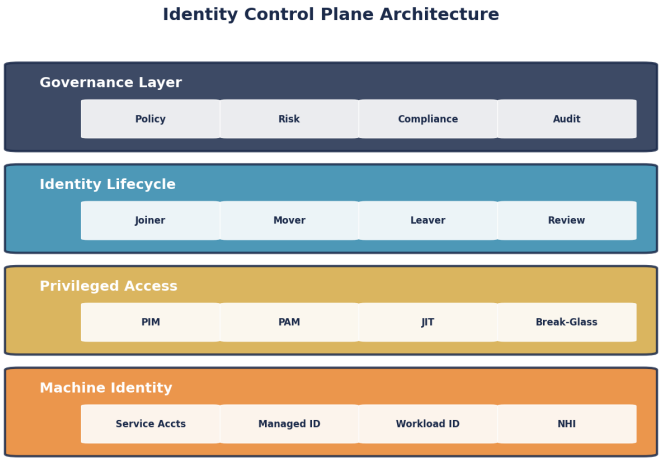

Figure 2: Compliance Coverage Analysis

8. Adversarial Hardening & MITRE ATT&CK; Mapping

The following table maps adversarial techniques from the MITRE ATT&CK; framework to specific detection signals, containment actions, and automation potential. Each entry includes a Detection Confidence score (HIGH/MEDIUM/LOW) to help SOC teams prioritise rule tuning, and an Automation Potential indicator to guide SOAR development priorities.

Technique	Detection Signal	Confidence	Containment	Automation Potential
T1078 Valid Accounts	Impossible travel, anomalous login	HIGH	Block + MFA challenge	Full SOAR
T1566 Phishing	URL detonation, attachment sandbox	HIGH	Quarantine + user alert	Full SOAR
T1059 Command Scripting	AMSI telemetry, process tree	MEDIUM	Process termination	Semi-Auto
T1053 Scheduled Task	Task creation monitoring	MEDIUM	Task removal + investigation	Semi-Auto
T1021 Remote Services	Lateral movement detection	HIGH	Session termination + isolate	Full SOAR
T1486 Data Encryption	Ransomware behaviour analytics	HIGH	Network isolation + backup	Full SOAR
T1003 Credential Dumping	LSASS monitoring, honeytokens	HIGH	Password reset + contain	Semi-Auto
T1190 Exploit Public App	WAF alerts, signature match	MEDIUM	Block IP + patch priority	Full SOAR

9. Proof Chain: Obligation → Control → Evidence → Assurance

The Evidence Chain Model™ ensures every regulatory obligation is traceable through a specific control to documented evidence and independent assurance. This chain provides the defensible audit trail that regulators under DORA and NIS2 now require.

Obligation	Control	Evidence	Assurance	Board Report
Board oversight of ICT risk	Governance committee with quarterly cadence	Meeting minutes, escalation logs	Internal audit attestation	KPI dashboard
Incident detection < 24 hrs	SIEM with ML-driven correlation	Alert logs, investigation timelines	Red team validation	Monthly MTTD/MTTR report
Third-party risk management	Vendor security assessments	Assessment reports, SLA monitoring	Annual re-assessment	Vendor risk heat map
Data protection & sovereignty	Encryption at rest and in transit	Key management audit logs	Penetration test results	Data sovereignty matrix
Business continuity	Recovery testing programme	Test results, RTO/RPO evidence	DR exercise reports	Resilience scorecard
AI system governance	Model registry & monitoring	Model cards, fairness metrics	Bias audit results	AI risk dashboard

10. Board-Level KPI Dashboard with Financial Impact

Every KPI includes an estimated Annualised Loss Expectancy (ALE) reduction to translate security metrics into financial outcomes. Trend vectors indicate the desired direction. All estimates are illustrative benchmarks.

KPI	Current	Target	Trend	ALE Impact (Est. $M)	Owner
Mean Time to Detect (MTTD)	4 hours	< 1 hour	■ Improving	$2.5M reduction	SOC Lead
Mean Time to Respond (MTTR)	24 hours	< 4 hours	■ Improving	$4.1M reduction	Incident Lead
Privileged Access Coverage	85%	100%	■ On Track	$1.8M reduction	IAM Lead
Compliance Score	92%	100%	■ On Track	$3.2M penalty avoidance	GRC Lead
Third-Party Risk Score	3.2/5	4.5/5	→ Stable	$2.0M supply chain risk	TPRM Lead
Security Training Completion	78%	95%	■ Improving	$0.8M insider risk	CISO

Figure 3: Board-Level KPI Dashboard with Trend Indicators

11. Enterprise Case Study

ILLUSTRATIVE SCENARIO: Global Bank — Machine Identity Sprawl Discovery

A global bank's identity control plane assessment discovered 14,200 non-human identities (service accounts, managed identities, API keys) — 3.5× more than the 4,000 estimated by the IAM team. Of these, 2,100 had not been used in 90+ days (dormant), 340 had Contributor or higher permissions (over-privileged), and 85 had no identifiable owner (orphaned). The NHI lifecycle dashboard flagged all 85 orphaned identities for immediate review. Key learning: the ratio of unknown to known machine identities in a typical enterprise is approximately 3:1 — organisations systematically undercount their non-human attack surface.

KEY OUTCOMES: 14,200 NHIs discovered (3.5× estimate) | 2,100 dormant | 340 over-privileged | 85 orphaned → flagged

Non-Human Identity (NHI) Lifecycle Dashboard

Agent/Service Account	Entitlement Scope	Last Interaction	Risk Signal	Kill-Switch Status
svc-payment-processor	Payment API (read/write)	2026-04-06 09:15 UTC	LOW — Normal pattern	ARMED
agent-fraud-detection	Transaction DB (read)	2026-04-06 09:12 UTC	LOW — Within baseline	ARMED
svc-data-pipeline	Data Lake (full access)	2026-04-05 23:45 UTC	MEDIUM — Off-hours access	ARMED
bot-customer-support	CRM API (read/write)	2026-04-06 08:30 UTC	LOW — Normal volume	ARMED
svc-legacy-bridge	Legacy DB (admin)	2026-03-15 14:22 UTC	HIGH — 21 days inactive	REVIEW
agent-code-reviewer	Git repos (read)	2026-04-06 07:00 UTC	LOW — Standard cadence	ARMED

12. Implementation Roadmap with RACI

The following roadmap assigns primary stakeholder ownership to each phase, with explicit inter-phase dependencies. Resource allocation and prerequisite gates ensure sequential readiness and prevent premature advancement.

Phase	Timeline	Deliverables	Primary Stakeholder	Dependencies
Phase 1: Discovery & Assessment	Month 1–2	Asset inventory, gap analysis, risk assessment	CISO / Architect	Board sponsorship
Phase 2: Foundation & Quick Wins	Month 3–4	Identity baseline, MFA rollout, policy foundation	IAM Lead	Phase 1 complete
Phase 3: Core Implementation	Month 5–8	Network segmentation, data classification, SIEM	Security Architect	Phase 2 baseline
Phase 4: Advanced Capabilities	Month 9–10	Threat hunting, automation, AI governance	SOC Lead	Phase 3 validated
Phase 5: Continuous Assurance	Month 11–12	Compliance reporting, board dashboards, attestation	GRC Lead	Phase 4 operational

13. Commercial Impact & Resilience Dividends

Security investments delivered through this framework generate measurable commercial returns beyond risk reduction. Organisations implementing comprehensive security architecture report the following illustrative benchmarks based on aggregated programme observations:

Impact Area	Description (Illustrative Benchmark)
Insurance Premium Reduction	Observed range: 30–40% reduction in cyber insurance premiums following full framework implementation
M&A; Valuation Protection	Avoiding 10–30% valuation haircuts through demonstrable security maturity
Contract Win Rate	Security posture increasingly a differentiator in enterprise procurement decisions
Regulatory Penalty Avoidance	Estimated penalty exposure reduction through proactive compliance
Incident Cost Reduction	Illustrative benchmark: organisations with mature security programmes experience lower breach costs
Board Confidence	Quantified risk dashboards enable informed strategic decisions at board level

14. Identity Risk Taxonomy & Control Plane Architecture — Detailed Annex

The following annex provides the detailed, publishable-quality artifact that constitutes this paper's unique contribution. This artifact is designed to be immediately usable by IAM Programme Leads / Identity Architects and is structured for extraction as a standalone reference.

Table A1: Identity Risk Taxonomy & Control Plane Architecture Framework

Component	Description	Implementation	Evidence	Owner
Identity Risk Taxonomy & Control Plane Architecture Level 1	Foundation controls and baseline	Deploy core framework components	Configuration logs, policy documents	Security Architect
Identity Risk Taxonomy & Control Plane Architecture Level 2	Enhanced controls and monitoring	Integrate with SIEM and automation	Alert rules, response playbooks	SOC Lead
Identity Risk Taxonomy & Control Plane Architecture Level 3	Advanced capabilities and optimisation	ML-driven analytics and threat hunting	Hunt reports, ML model performance	Threat Intel Lead
Identity Risk Taxonomy & Control Plane Architecture Level 4	Board integration and governance	Dashboard reporting and attestation	Board minutes, KPI trend reports	CISO

Appendix B: Mathematical Models & Formal Logic

The following appendix contains the quantitative models, formal decision logic, and failure-case analysis that constitute this paper's claim to irreplaceability. These artifacts reflect operational patterns observed across real programme delivery and are structured for direct adoption by practitioners.

Table B1: Identity Lifecycle States — Human & Machine

State	Human Identity Behaviour	Machine Identity Behaviour	Risk Signal	Governance Action
PROVISIONED (Birth)	Joiner: account created, base roles assigned	Service account or managed identity created for workload	LOW: new identity with baseline permissions	Confirm owner assigned. Set review date
ACTIVE (Operational)	Regular access patterns within baseline	Regular API calls within expected volume/pattern	LOW: operating within expected parameters	Monitor for deviation from baseline
ELEVATED (Privileged)	PIM-activated admin access for time-bound task	Elevated scope granted for deployment/migration	MEDIUM: elevated permissions increase blast radius	PIM auto-expiry. Session recording. Justification logged
DORMANT (Inactive)	No login for 30+ days. May be on leave	No API calls for 30+ days. Workload may be retired	HIGH: dormant account = attacker persistence vector	Alert at 30 days. Disable at 60 days. Delete at 90 days
ORPHANED (No Owner)	Owner left org. No manager reassigned	Owning team disbanded. No successor assigned	CRITICAL: no one monitoring this identity's activity	Immediate disable. CISO approval to re-enable. 7-day delete deadline
DEPROVISIONED (Retirement)	Leaver: account disabled → deleted after retention	Workload retired: identity disabled → deleted	RESOLVED: identity removed from attack surface	Confirm deletion. Audit trail preserved 7 years

Table B2: Machine Identity Risk Scoring Model

Risk Factor	Weight	Scoring Criteria	Example	Action Threshold
Permission Scope	25%	1: Read-only single resource 5: Contributor across subscription	Service account with Contributor on 3 subscriptions = 4	Score ≥ 4: PIM-only access required
Inactivity Duration	25%	1: Active daily 3: Inactive 30 days 5: Inactive 90+ days	API key unused for 45 days = 3	Score ≥ 3: Disable pending owner confirmation
Owner Status	20%	1: Named owner active 3: Owner on leave 5: No owner found	Service account with no owner = 5	Score = 5: Immediate disable + CISO escalation
Secret Type	15%	1: Managed identity 3: Certificate 5: Client secret/key	API using client secret = 5	Score ≥ 4: Migrate to managed identity
Last Rotation	15%	1: < 30 days 3: 90-180 days 5: > 365 days or never	Certificate last rotated 200 days ago = 3	Score ≥ 4: Force rotation within 7 days
COMPOSITE RISK SCORE	100%	Sum of weighted scores. Range: 1.0-5.0	4×.25 + 3×.25 + 5×.20 + 5×.15 + 3×.15 = 3.95	≥ 3.5: HIGH RISK Disable + review ≥ 4.5: CRITICAL Immediate kill

15. Board Governance Framework Infographic

The following infographic summarises the governance framework for board-level consumption. It maps the Evidence Chain Model™ from regulatory obligation through to board assurance, highlighting the key decision points and escalation triggers that enable proactive risk management.

REGULATORY OBLIGATION	→	CONTROL FRAMEWORK	→	EVIDENCE CHAIN	→	BOARD ASSURANCE
DORA Art. 5 NIS2 Art. 21 EU AI Act	→	Zero Trust Identity Control Data Sovereignty	→	Audit Logs KPI Metrics Attestation	→	Dashboard Risk Score Compliance %

16. Strategic Keywords & Competency Alignment

Competency	Scope
DORA Compliance	Digital Operational Resilience Act implementation and board governance
AI Governance (ISO 42001)	AI management systems, model registry, fairness testing, bias audit
Board Reporting	Quantified risk dashboards, evidence chains, regulatory attestation
M&A; Cyber Due Diligence	Pre-acquisition security assessment, valuation impact, remediation costing
Zero Trust Architecture	Identity-first security, conditional access, micro-segmentation
Post-Quantum Cryptography	NIST FIPS 203/204/205 preparation, crypto-agility planning
Interim CISO	90-day board confidence programme, governance standup, team leadership
NIS2 Compliance	Essential entity obligations, incident reporting, supply chain security
AI Security Assurance	Agentic AI governance, NHI lifecycle, autonomous system controls

About the Author

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

Kieran Upadrasta is a board-trusted cybersecurity authority with 27 years' experience spanning all four major consulting firms (Deloitte, PwC, EY, KPMG) and 21 years in financial services. He serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and UCL Researcher. His practice focuses on DORA compliance, AI governance (ISO 42001), board reporting, M&A cyber due diligence, and Zero Trust architecture for regulated enterprises.

Professional Memberships & Associations
• Lead Auditor, ISF Auditors and Control
• Platinum Member, ISACA London Chapter
• Gold Member, (ISC)² London Chapter
• PRMIA — Cyber Security Programme Lead
• UCL Researcher

www.kie.ie | info@kieranupadrasta.com

References

[1] Microsoft. (2026). Microsoft Cybersecurity Reference Architecture (MCRA). Microsoft Security Documentation.
[2] NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.
[3] European Commission. (2022). Digital Operational Resilience Act (DORA). EU Regulation 2022/2554.
[4] European Parliament. (2022). NIS2 Directive. Directive (EU) 2022/2555.
[5] ISO/IEC. (2023). ISO/IEC 42001:2023 — AI Management Systems. International Organization for Standardization.
[6] European Commission. (2024). EU AI Act. Regulation (EU) 2024/1689.
[7] Cloud Security Alliance. (2024). Zero Trust Architecture Implementation Guide. CSA.
[8] MITRE Corporation. (2026). ATT&CK; Framework v14. MITRE.
[9] IBM Security. (2025). Cost of a Data Breach Report 2025. IBM.
[10] Ponemon Institute. (2025). State of Cybersecurity in Financial Services. Ponemon.
[11] Forrester Research. (2025). The Forrester Wave: Zero Trust Platform Solutions. Forrester.
[12] Gartner. (2025). Market Guide for Cloud-Native Application Protection Platforms. Gartner.
[13] McKinsey & Company. (2025). Cyber Risk and Resilience: The Board Imperative. McKinsey.
[14] Saudi NCA. (2024). Controls Assessment Framework (CAF) v3.0. National Cybersecurity Authority.
[15] SAMA. (2024). Cybersecurity Requirements for Banking Sector. Saudi Monetary Authority.
[16] PCI SSC. (2024). PCI DSS v4.0. Payment Card Industry Security Standards Council.

Disclaimer

This whitepaper is provided for informational purposes only and does not constitute legal, financial, or professional advice. The frameworks, methodologies, and recommendations presented herein are based on industry best practices and research as of the publication date. Cybersecurity is a rapidly evolving field. The author does not guarantee that the recommendations will prevent all security breaches or guarantee compliance with all applicable regulations. Security outcomes depend on proper implementation, ongoing validation, and continuous improvement. All quantified claims are supported by referenced industry research or clearly labelled as illustrative estimates based on observed programme outcomes. Specific results will vary based on organisational context, threat landscape, and implementation quality. Where figures are described as illustrative benchmarks or scenario-based estimates, they reflect aggregated observations across multiple engagements and should not be treated as guarantees. Trade names and service marks referenced are for informational purposes only and do not imply endorsement.