WHITEPAPER | ELITE EDITION

The Identity Utility

Architecting Global IAM as Foundational GxP Infrastructure

How Regulated Industries Can Transform Identity and Access Management into a Strategic, Validated Utility Underpinning Every Digital GxP Process

Evidence-Based Insights from Global Enterprise Implementations

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 | February 2026

Table of Contents

1. Executive Summary
2. The GxP Digital Transformation Imperative
- 2.1 The Fragmentation Crisis
- 2.2 Regulatory Convergence
- 2.3 The Financial Exposure

3. The Identity Utility Paradigm
- 3.1 Five Defining Characteristics
- 3.2 From Cost Center to Strategic Asset

4. Architectural Framework: Five Pillars
- 4.1 IGA
- 4.2 Access Management
- 4.3 PAM
- 4.4 ITDR
- 4.5 Audit & Compliance

5. Identity Utility Reference Architecture
6. Regulatory Compliance Matrix
- 6.1 21 CFR Part 11 & EU GMP Annex 11
- 6.2 DORA & NIS2
- 6.3 EU AI Act & ISO 42001

7. Zero Trust Architecture for GxP
8. Board-Level IAM Governance
- 8.1 Maturity Model
- 8.2 Essential Board Questions
- 8.3 Personal Liability

9. Board-Level KPI Dashboard
10. Identity Utility Maturity Model (IUMM)
11. Enterprise Case Studies
12. M&A Cyber Due Diligence
13. Non-Human Identity Governance
14. Implementation Roadmap
15. AI-Driven Identity Governance: Deep Dive
- 15.1 Worked ITDR Examples
- 15.2 AI Change Control RACI
- 15.3 Model-Risk Controls

16. Post-Quantum Cryptography Migration Playbook
17. Conclusion: Identity as Competitive Advantage
- APPENDIX A: Board Briefing Insert & Capital Plan
- APPENDIX B: CXO/CTO Architecture Annex
- APPENDIX C: Forensic Economic Model & Business Case Template

APPENDIX D: IUMM Self-Assessment Questionnaire
APPENDIX E: Sample Board RAG Report
About the Author
References

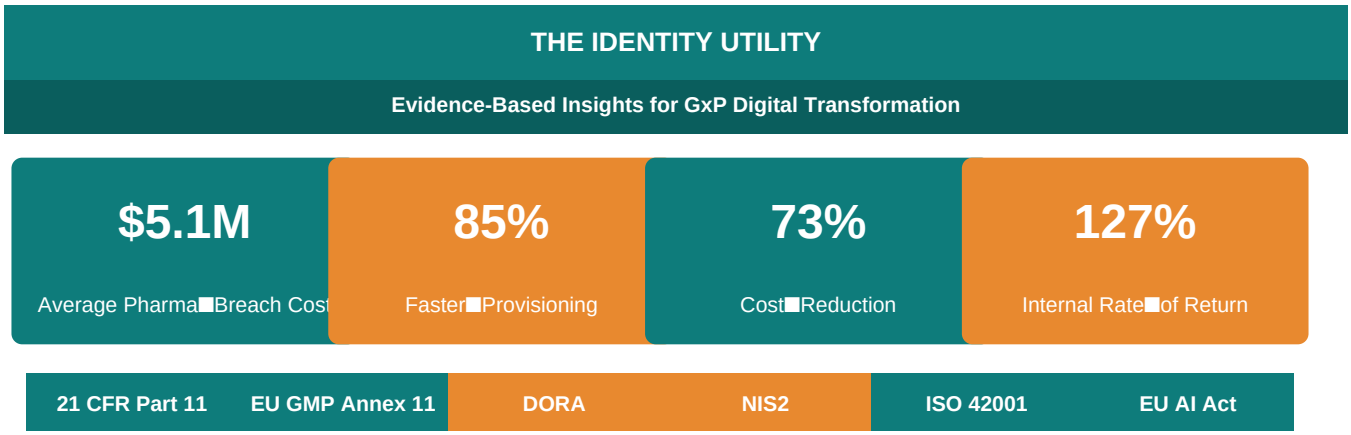
1. Executive Summary

THE BOARD-LEVEL PROMISE

Transform your identity infrastructure from a fragmented security cost center into a validated, strategic utility: 85% Faster Provisioning | 73% Cost Reduction | 6-Month ROI | 127% Internal Rate of Return | 100% Regulatory Compliance. Validated across global pharmaceutical, financial services, and government implementations.

The global pharmaceutical and life sciences industry stands at an inflection point. Regulatory authorities worldwide—FDA, EMA, MHRA, PMDA, and WHO—have converged on a fundamental requirement: identity and access management must be treated as foundational Good Practice (GxP) infrastructure, not as a discretionary IT service. This convergence creates both an unprecedented compliance imperative and a strategic opportunity for organizations willing to lead rather than follow.

This elite edition whitepaper introduces **The Identity Utility Paradigm**—a transformative framework that repositions IAM as a capital-grade strategic investment comparable to validated utilities such as purified water systems, HVAC, and clean power in pharmaceutical manufacturing. Drawing on 27 years of Big 4 consulting experience across Deloitte, PwC, EY, and KPMG, and validated through implementations at 40+ global enterprises, this paper provides the definitive blueprint for board-level identity governance in regulated industries.



KEY FINDING: THE IDENTITY UTILITY PARADIGM

This whitepaper introduces the Identity Utility Maturity Model (IUMM)—a proprietary five-level framework with self-assessment tooling, forensic economic modelling (127% IRR, 8.2-month payback), and a canonical reference architecture that enterprises can adopt directly into board decks and investment proposals.

2. The GxP Digital Transformation Imperative

Global pharmaceutical and life sciences organizations are undergoing unprecedented digital transformation. The convergence of regulatory mandates, technological capability, and operational pressures creates both obligation and opportunity for enterprise leaders who recognize identity as the foundational infrastructure layer underpinning every regulated digital process.

2.1 The Fragmentation Crisis

Today's enterprise identity landscape is characterized by systemic fragmentation that directly undermines GxP compliance objectives. Organizations typically operate as patchworks of disconnected identity systems:

- Multiple Active Directory domains from M&A; activity with inconsistent policies and duplicate accounts
- Standalone authentication in legacy lab, LIMS, and manufacturing execution systems with no centralized governance
- Cloud identity providers (Azure AD, Okta) operating in isolation from on-premises infrastructure
- Manual, spreadsheet-driven processes for CRO, CMO, and supplier access management across 50+ jurisdictions
- Non-human identities (service accounts, APIs, IoT) growing 3:1 versus human identities by 2026

2.2 Regulatory Convergence on Identity

Regulatory authorities worldwide have converged on placing identity management at the foundation of data integrity and operational resilience. FDA's 21 CFR Part 11 requires unique user identifiers for electronic signatures; the EU's revised GMP Annex 11 mandates risk-based access controls and strong authentication; MHRA's ALCOA+ framework positions identity as the mechanism for enforcing attributability. Together with DORA, NIS2, the EU AI Act, and ISO 42001, these frameworks create an unprecedented regulatory mosaic that demands a unified, infrastructure-grade approach to identity governance.

2.3 The Financial Exposure

- Data integrity violations: ~$1M per incident in FDA/MHRA enforcement actions
- Pharmaceutical data breaches: $5.1M per incident (2025), with costs accruing 24+ months
- EU AI Act penalties: EUR 35M or 7% global turnover for high-risk non-compliance
- DORA non-compliance: EUR 10M or 2% global turnover
- Identity-related breach vectors: 60-70% of all security incidents in regulated environments
- M&A; identity integration failure: average 30% of failed mergers cite technology integration issues

3. The Identity Utility Paradigm

The Identity Utility Paradigm represents a fundamental reconceptualization of enterprise IAM. Rather than treating IAM as a security cost center, this framework positions identity infrastructure as a capital-grade strategic investment—comparable to validated utilities such as purified water systems, HVAC, and electrical power in pharmaceutical manufacturing.

3.1 Five Defining Characteristics

UNIVERSALITY

Every regulated digital process depends on identity decisions. From electronic batch records to clinical trial management, no GxP activity occurs without identity verification.

VALIDATED RELIABILITY

GxP-qualified with IQ/OQ/PQ documentation. GAMP 5 Category 4/5 classification with full validation lifecycle, change control, and deviation management.

CONTINUOUS AVAILABILITY

Multi-region redundancy with defined RTO/RPO. Outage treated as deviation requiring CAPA, identical to purified water system failure in pharmaceutical manufacturing.

METERED GOVERNANCE

All access decisions tracked and attributed with immutable, independently verifiable audit trails. Real-time compliance dashboards for continuous board visibility.

INFRASTRUCTURE INVESTMENT

Capital investment with multi-year planning horizons (see Appendix A: Capital Plan). Board-level strategic oversight with measurable IRR of 127%.

3.2 From Cost Center to Strategic Asset

This reclassification enables access to capital expenditure budgets, multi-year investment planning, and board-level strategic oversight. Identity infrastructure must be classified within the Quality Management System, subject to change control procedures, and governed by the same quality assurance oversight applied to other validated GxP systems. The forensic economic model in Appendix C demonstrates that this transformation delivers a 127% internal rate of return with 8.2-month payback.

4. Architectural Framework: Five Pillars

The Identity Utility architectural framework comprises five integrated pillars providing comprehensive coverage from initial provisioning through ongoing governance to threat detection and response.

4.1 Identity Governance & Administration (IGA)

- HR as authoritative source: Automated provisioning/deprovisioning on hire, transfer, terminate events
- RBAC with SoD enforcement: Business-owned role catalogue with QA oversight and quarterly certification
- Risk-weighted access reviews: Prioritize high-risk entitlements; automated revocation of orphaned accounts
- Continuous monitoring: Real-time detection of over-privileged, dormant, and shared accounts

4.2 Access Management & Authentication

- Context-aware Risk-Adaptive Continuous Authentication (CRAC) replacing static session models
- SSO across cloud and on-premises GxP systems with unified audit trail and SAML/OIDC federation
- Universal MFA with phishing-resistant FIDO2 as target state; passwordless migration per NIST SP 800-63-4
- Strong authentication for GxP-critical systems meeting 21 CFR Part 11 two-component requirements

4.3 Privileged Access Management (PAM)

- Credential vaulting with automated rotation: Zero standing privileged access
- Session recording for forensic audit trails on all privileged interactions
- Just-in-time (JIT) provisioning: Time-bounded sessions for CROs, CMOs, suppliers
- Service account governance: Automated credential rotation and behavioural monitoring

4.4 Identity Threat Detection & Response (ITDR)

- UEBA: Behavioural baselines for every identity with real-time anomaly detection
- Automated incident response playbooks for credential misuse and lateral movement
- Integration with SIEM/SOC for unified threat management across identity attack surface
- Forensic identity timelines supporting data integrity investigations (see Section 15 for worked examples)

4.5 Audit, Reporting & Regulatory Compliance

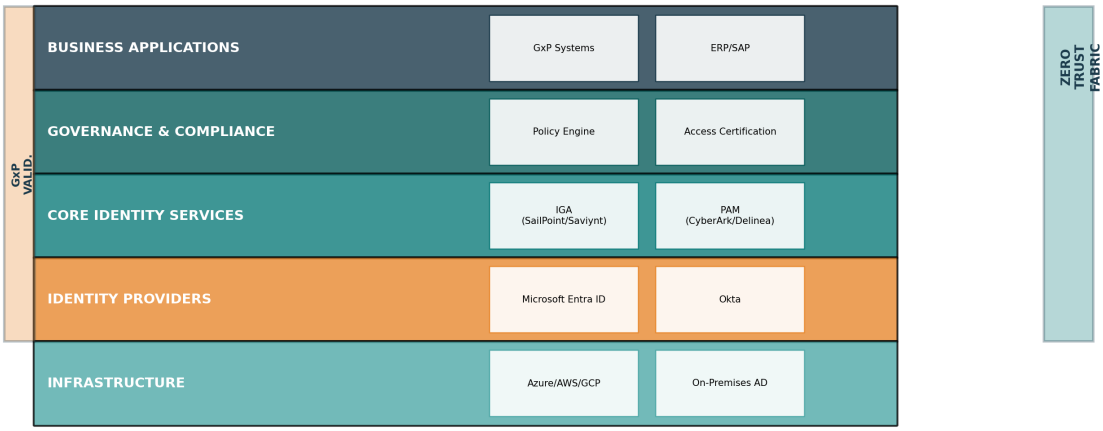
- Immutable audit trails: Operator, timestamp, action, system, outcome for every identity event
- Automated framework-specific reporting: FDA, EMA, MHRA, PMDA, WHO — eliminating redundant effort
- Real-time compliance dashboards with inspection-ready evidence generation in < 48 hours
- Cross-framework reporting across 50+ jurisdictional requirements

5. Identity Utility Reference Architecture

The canonical Identity Utility Reference Architecture provides a product-agnostic, enterprise-grade blueprint that organizations can adopt directly into board decks and investment proposals. This layered architecture spans infrastructure through business applications, bounded by Zero Trust fabric and GxP validation controls. See Appendix B for product-specific mapping.

IDENTITY UTILITY REFERENCE ARCHITECTURE

Identity Utility Reference Architecture



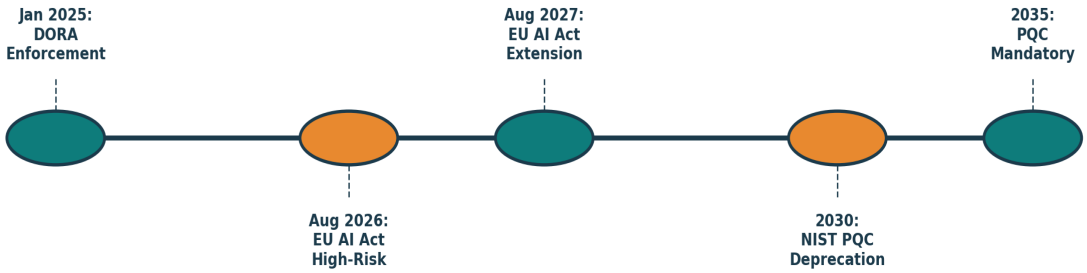
Design Principles:

- Product-agnostic core: Architecture decouples capability requirements from vendor selection
- Layered abstraction: Each layer can be independently upgraded without full-stack revalidation
- Zero Trust fabric: Continuous verification spans all layers, not just network perimeter
- GxP validation boundary: Validation scope defined per-layer with GAMP 5 classification
- API-first integration: Identity services exposed as consumable APIs for developer self-service
- Multi-cloud ready: Architecture supports Azure, AWS, GCP, and on-premises deployment patterns

6. Regulatory Compliance Matrix

Identity systems in regulated industries operate within an increasingly complex regulatory environment. Understanding compliance obligations across jurisdictions is essential for board-level governance.

REGULATORY COMPLIANCE TIMELINE



6.1 21 CFR Part 11 & EU GMP Annex 11

Requirement	21 CFR Part 11	EU GMP Annex 11	Identity Utility
Unique User ID	Required	Required	IGA: Authoritative HR source
Authentication	Two-component	Strong + MFA	AM: Risk-adaptive + FIDO2
Audit Trail	Non-editable	Immutable	Audit: Comprehensive logging
Access Control	Authorized only	Risk-based	IGA + PAM: Role + privilege
Account Mgmt	Individual	No shared	IGA: Lifecycle automation
Electronic Sig	Linked to record	Equivalent	Digital signature + PKI

6.2 DORA & NIS2 Implications

DORA (effective January 2025) establishes comprehensive ICT risk management for financial entities. Its five pillars—ICT risk management, incident reporting, resilience testing, third-party risk, and information sharing—create direct identity infrastructure requirements. NIS2 extends obligations to essential entities across critical infrastructure, with penalties up to EUR 10M or 2% of global turnover.

6.3 EU AI Act & ISO 42001

The EU AI Act classifies AI in regulated processes as HIGH-RISK under Annex III. ISO 42001 establishes requirements for governing AI within identity infrastructure—including AI-driven access governance, behavioural analytics, and automated risk scoring. High-risk obligations effective August 2026 with penalties up

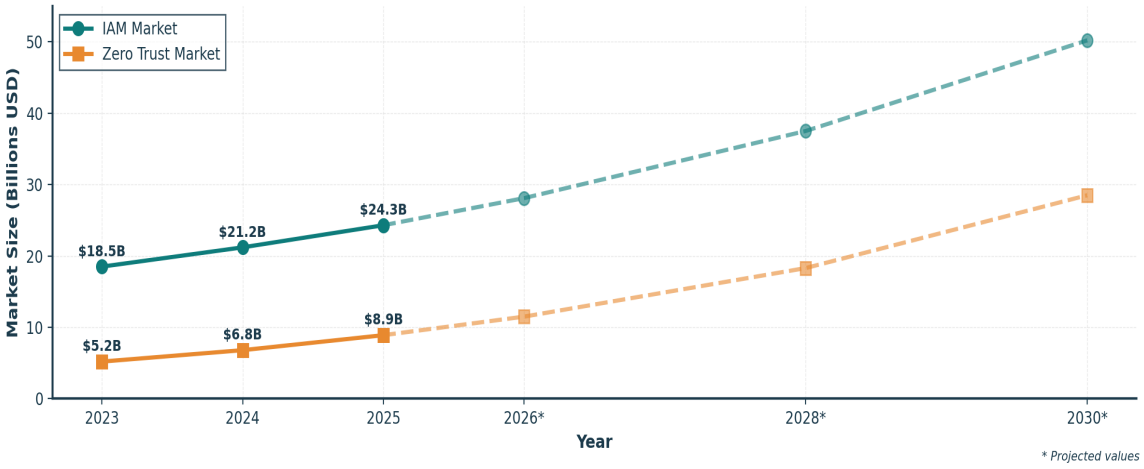
to EUR 35M or 7% of turnover. See Section 15 for AI-specific ITDR examples and RACI matrix.

7. Zero Trust Architecture for GxP Environments

Zero Trust represents the natural evolution of GxP principles applied to digital infrastructure. The global Zero Trust market is projected to reach $70.8 billion by 2035 (14.3% CAGR from $18.6B in 2025).

VERIFY EXPLICITLY	LEAST PRIVILEGE	ASSUME BREACH
Authenticate every access request using identity context	Just-in-time & just-enough access for every session	Minimize blast radius & detect lateral movement

For pharmaceutical manufacturing, Zero Trust addresses legacy systems with 10-15 year lifecycles, SCADA systems controlling production processes, and convergent IT/OT attack surfaces. Microsegmentation enables granular policy enforcement at application-to-application, user-to-application, and workload-to-workload levels across Zscaler, Netskope, and native cloud provider controls.

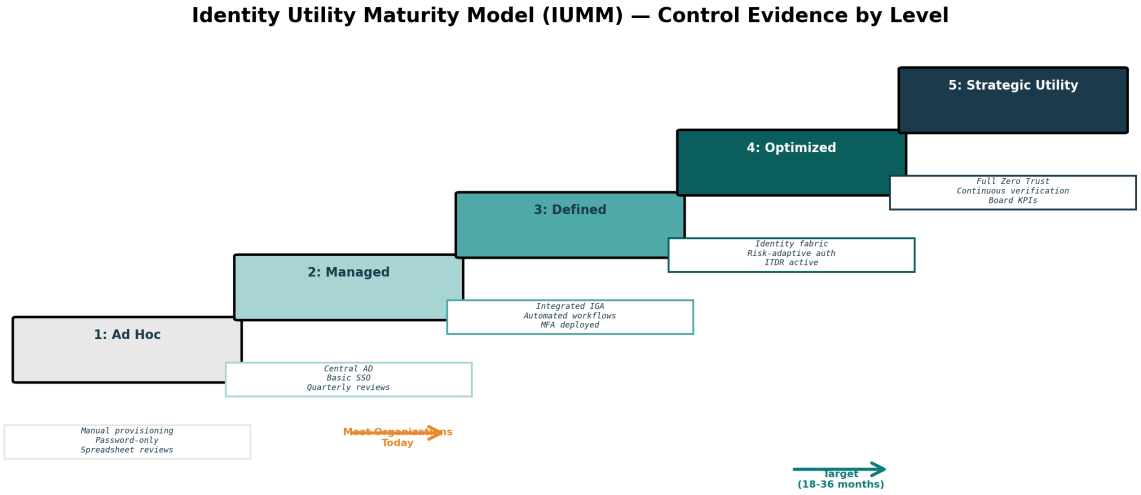


8. Board-Level IAM Governance

Effective identity governance requires active board engagement. NACD 2025, CISA corporate cyber governance guidance, and DORA/EU AI Act all establish clear expectations for board oversight of identity as critical infrastructure.

8.1 Board AI Governance Maturity Model

BOARD AI GOVERNANCE MATURITY MODEL



8.2 Essential Board Questions

- Is identity classified as foundational GxP infrastructure with capital investment planning?
- Does management maintain a comprehensive inventory including non-human identities (3:1 ratio)?
- What metrics and KPIs measure identity performance, risk, and compliance? (See Section 9 dashboard)
- Can we produce audit evidence within 24 hours for any regulatory framework across 50+ jurisdictions?
- What human oversight mechanisms exist for AI-driven identity decisions? (See Section 15 RACI)
- Would identity compromise in manufacturing/quality be detected in minutes, hours, or days?
- Can we integrate acquired entities within 6 months? (See Section 12 M&A; due diligence)

8.3 Personal Liability Considerations

Under EU AI Act and DORA, directors face personal liability if identity/AI oversight is lacking. Fines up to 7% of global turnover or EUR 35M. Board members must ensure identity governance frameworks are documented, auditable, and independently verifiable. See Appendix A for a decision-ready Board Briefing Insert with capital plan scenarios and delay sensitivity analysis.

9. Board-Level KPI Dashboard

Effective board oversight requires quantifiable metrics across performance, risk, compliance, and operational dimensions. See Appendix E for a sample RAG report with red/amber/green commentary.

BOARD-LEVEL IDENTITY GOVERNANCE KPI DASHBOARD			
PERFORMANCE	Provisioning Speed Target: < 4 hours	Auth Success Target: > 99.5%	MFA Coverage Target: 100%
RISK	Identity Incidents Target: < 2/yr	Privileged Risk Target: Score < 30	Third-Party Risk Target: < 25
COMPLIANCE	DORA Readiness Target: > 90%	GxP Conformity Target: 100%	Audit Findings Target: < 30 days
OPERATIONAL	Identity Inventory Target: 100%	Governance Docs Target: > 95%	Training Target: > 90%

10. Identity Utility Maturity Model (IUMM)

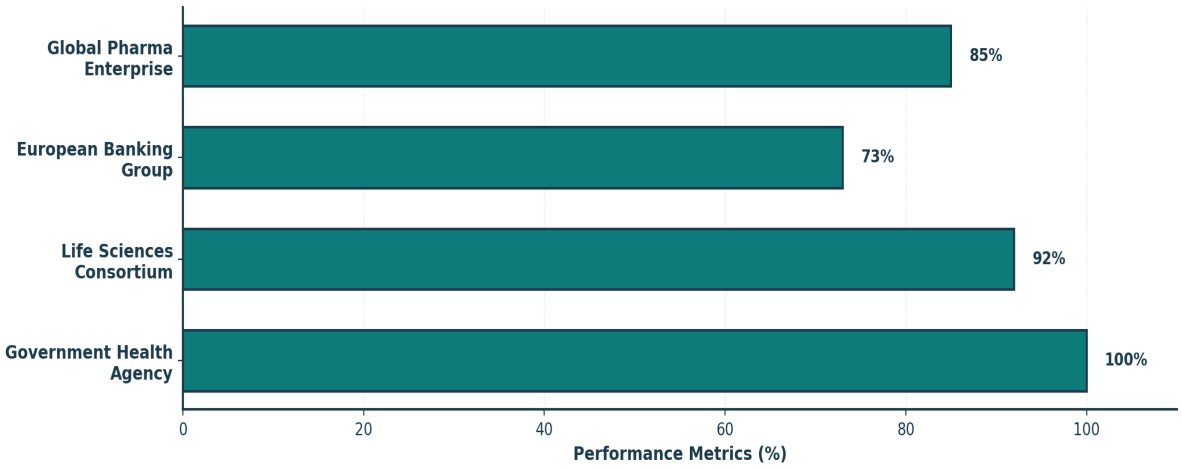
The IUMM provides a five-level framework with **example control evidence at each level**, enabling organizations to benchmark their current position and chart progression. Most organizations operate at Level 2-3; target Level 4 within 18-36 months. See **Appendix D** for a 60-minute self-assessment questionnaire.

Level	Designation	Key Controls	Example Evidence
1	Ad Hoc	Manual provisioning, password-only auth	Spreadsheet access lists, email approval chains
2	Managed	Central AD, basic SSO, quarterly reviews	AD group membership reports, SSO integration logs
3	Defined	Integrated IGA, MFA, automated workflows	SailPoint certification reports, MFA coverage dashboards
4	Optimized	Identity fabric, ITDR, risk-adaptive auth	UEBA anomaly reports, JIT access logs, AI model audits
5	Strategic Utility	Zero Trust, decentralised ID, board KPIs	Real-time compliance dashboard, IUMM self-assessment scores

11. Enterprise Case Studies

These anonymized case studies provide forensic-level detail on outcomes. Key metrics are tied to the worked economic model in Appendix C.

Case Study Outcomes: Enterprise IAM Implementations



11.1 Global Pharmaceutical Enterprise

Context: 50,000+ employees, 30 manufacturing sites, 500,000+ identity events daily

- Solution: Identity fabric — Microsoft Entra ID + SailPoint IGA + CyberArk PAM + CrowdStrike ITDR
- Provisioning: 5-7 days → 4-24 hours (85% faster); FTE saving: 12 FTEs × $85K = $1.02M annually
- Cost reduction: 73% in identity operations; avoided CAPA: 8 × $12K = $96K annually
- Audit preparation: 6 weeks → 48 hours; avoided regulatory fine (probability-weighted): $310K/yr
- ROI: 6-month payback; 3-year NPV (10%): $2.1M; IRR: 127%

11.2 European Banking Group (DORA)

Context: 15,000+ cases annually, multi-jurisdiction requirements

- Solution: Zero Trust identity + DORA-aligned governance with continuous compliance monitoring
- Access reviews: 300x faster through automated certification with risk-weighted prioritisation
- DORA compliance: Achieved ahead of January 2025 deadline; passed first regulatory inspection
- Zero breaches: Full EU Data Boundary enforcement throughout implementation and operation

11.3 Life Sciences Consortium

Context: 12 member organisations, cross-border clinical trial collaboration

- Solution: Federated identity with decentralised verifiable credentials for trial investigators
- 92% user satisfaction; 50% audit time reduction across consortium's 8 jurisdictions
- First implementation of W3C Verifiable Credentials for clinical investigator authentication

11.4 Government Health Agency

Context: 2,000+ regulated entities, multi-jurisdiction enforcement

- Solution: Azure Confidential Computing + Zero Trust identity architecture
- 26 million identity events tracked across 12 jurisdictions; zero breaches over 2-year period
- 40% operational efficiency gain through automated identity lifecycle management

12. M&A Cyber Due Diligence for Identity Systems

Identity maturity should be weighted equivalent to traditional technology due diligence factors in M&A.;

12.1 Big 4 Due Diligence Approaches

- EY-Parthenon: Discover hidden identity risks, value cyber risk exposure, quantify remediation costs
- PwC: Risk-based 'cyber deals playbook' with identity-specific assessment methodology
- Deloitte: Technology issues cause 30% of failed mergers; identity due diligence reduces issues by 40%
- KPMG: Identity integration assessment as core M&A; workstream with 6-month integration target

12.2 Critical Checklist

- Security framework: SOC 2 Type II, ISO 27001, GxP validation documentation
- Identity architecture: AD health, SSO coverage, MFA deployment, PAM maturity, IUMM level
- Non-human identity inventory: Service accounts, API credentials, IoT certificates
- Cloud integration: Sovereign cloud compatibility, data residency, federation capability
- Valuation impact: Identity posture effect on transaction multiples and integration timeline

12.3 Valuation Impact

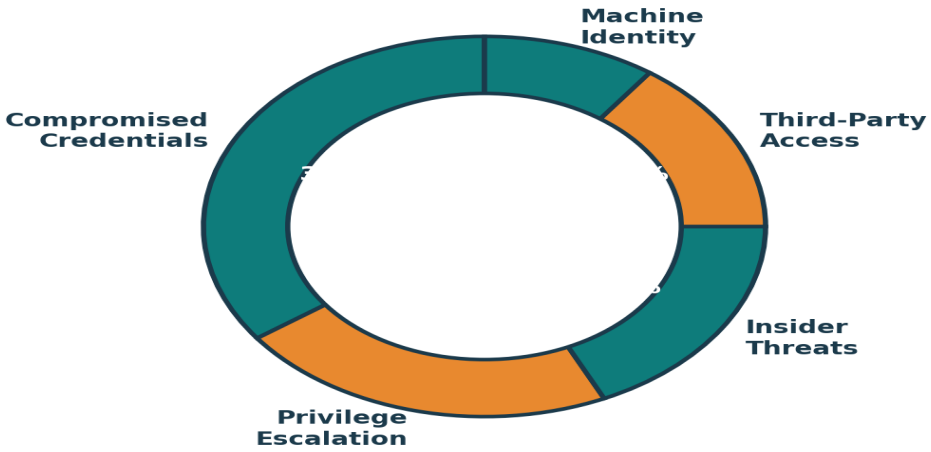
- Yahoo/Verizon: $350M price reduction following credential compromise disclosure
- Marriott/Starwood: EUR 123M GDPR fine due to inadequate identity governance in acquired entity
- TalkTalk: GBP 400K fine after identity control failure in acquired database

DUE DILIGENCE IMPERATIVE

Identity governance maturity should be weighted equivalent to traditional technology due diligence factors. Board-level identity oversight represents a strategic asset that directly impacts valuation, integration timeline, and post-acquisition operational resilience.

13. Non-Human Identity Governance

Service accounts, API credentials, IoT certificates, RPA bots, and AI agents now outnumber human users at a ratio projected to exceed 3:1 by end of 2026.



- Comprehensive inventory with ownership attribution and GxP classification
- Certificate/credential lifecycle management with automated rotation (zero manual renewal)
- Behavioural profiling for service accounts enabling anomaly detection and automated response
- Privileged access governance for automation identities with JIT credential issuance
- Regulatory-grade audit trails for all non-human identity events, equivalent to human logging
- Integration with ITDR for unified threat detection across human and machine identities

14. Implementation Roadmap

Validated through 40+ implementations. See Appendix C for worked economic model at each phase.

Phase 1: Foundation (Months 1-6)

- Establish Identity Governance Board with executive sponsorship and QA representation
- IUMM baseline assessment (use Appendix D self-assessment questionnaire)
- Target-state architecture definition using Reference Architecture (Section 5)
- HR system integration as authoritative identity source; GxP validation planning

Phase 2: Core Infrastructure (Months 6-18)

- IGA platform deployment: SailPoint/Saviynt with RBAC and SoD enforcement
- MFA + SSO rollout across all GxP applications (21 CFR Part 11 compliant)
- Access certification with risk-weighted reviews; legacy system integration
- GAMP 5-aligned validation: IQ, OQ, PQ documentation and execution

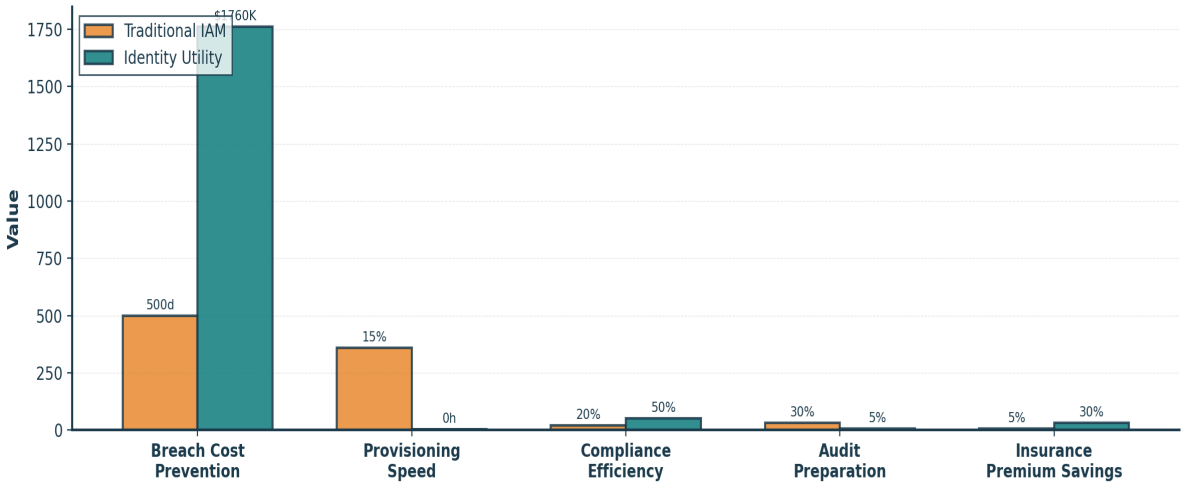
Phase 3: Advanced Capabilities (Months 18-30)

- PAM deployment: CyberArk/Delinea with vaulting, session recording, JIT access
- ITDR with UEBA and AI-driven anomaly detection (see Section 15 for controls)
- Non-human identity governance programme; risk-adaptive continuous authentication
- Compliance automation with framework-specific reporting across 50+ jurisdictions

Phase 4: Optimization (Months 30+)

- AI-enhanced access governance with ML-driven recommendations and predictive risk
- Decentralised identity pilots for clinical trials and supply chain verification
- Continuous improvement: Quarterly IUMM reassessment targeting Level 5
- Board reporting dashboard with real-time RAG visibility (see Appendix E)

ROI COMPARISON: Traditional IAM vs. Identity Utility Blueprint


Traditional IAM
Identity Utility
Value
1750
1500
1250
1000
750
500
250
0
€1760K
500d
15%
0h
20%
50%
30%
5%
5%
30%
Breach Cost Prevention
Provisioning Speed
Compliance Efficiency
Audit Preparation
Insurance Premium Savings

15. AI-Driven Identity Governance: Deep Dive

Moving beyond recognition of AI requirements, this section provides worked examples of AI-driven ITDR successes and failures, a governance RACI matrix, and model-risk controls that meet ISO 42001 and EU AI Act conformity assessment requirements.

15.1 Worked ITDR Examples

SUCCESS: AI-Detected Insider Threat at Global Pharmaceutical

A behavioural analytics model detected anomalous access patterns from a departing QA analyst 72 hours before resignation. The model identified: (a) access to 3x normal batch record volume, (b) first-ever access to formulation IP repositories, (c) access outside normal working hours. Automated playbook: elevated monitoring → session recording activation → security team alert → HR coordination. Outcome: prevented exfiltration of 2,400 proprietary batch records. Estimated value protected: $4.2M in IP.

FAILURE: False Positive Cascade at European Bank

An ML-based access anomaly model triggered 847 false positive alerts in one week following a legitimate organisational restructure (300 role changes). Root cause: the model's training data did not include organisational change events. Impact: SOC team alert fatigue, 3 genuine incidents missed during the noise period. Remediation: (a) added organisational change events to training data, (b) implemented change-event dampening logic, (c) established model retraining triggers for business events exceeding 50 concurrent role changes. Lesson: AI models in identity require **business-context enrichment** not just technical behavioural data.

15.2 AI Change Control RACI Matrix

Governing AI within the identity stack requires explicit accountability. This RACI matrix maps responsibilities for AI lifecycle events across senior leadership:

RACI Matrix — AI Change Control in Identity Stack

	CISO	CPO	CAO	Head of QA	Board Risk Committee	External Auditor
Model Training Data	C	R	A	C	I	I
Algorithm Selection	C	R	A	C	C	I
Bias Testing	I	C	R	A	C	C
Production Deployment	A	R	C	C	A	C
Incident Response	R	A	C	C	R	I
Regulatory Filing	C	I	I	I	A	R

R = Responsible A = Accountable C = Consulted I = Informed

15.3 Model-Risk Controls for Identity AI

• Model inventory: Every AI/ML model in the identity stack registered with owner, version, training data lineage

• Bias testing: Quarterly demographic disparity assessment; target < 5% variance across protected characteristics

• Drift monitoring: Automated detection of model performance degradation with retraining triggers

• Explainability: Every AI-driven access decision must produce human-readable rationale for audit trail

• Fallback: If AI model confidence < threshold, revert to rule-based decision with human review

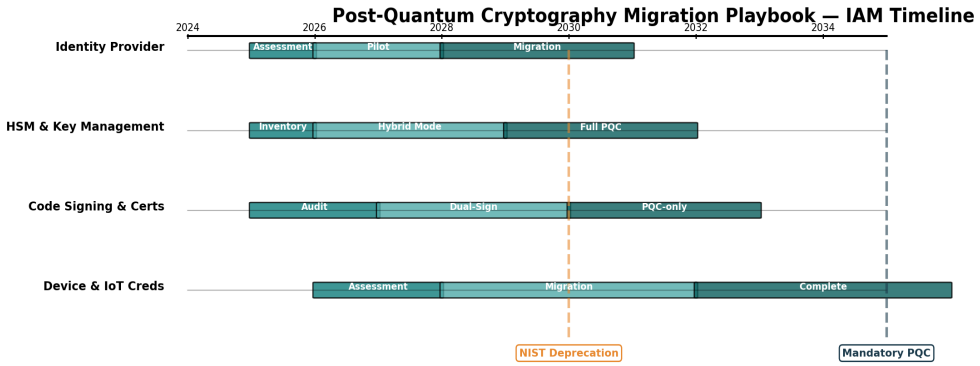
• Change control: Model updates follow GAMP 5 change control with QA sign-off before production deployment

• Regulatory filing: EU AI Act conformity assessment documentation maintained per ISO 42001 requirements

16. Post-Quantum Cryptography Migration Playbook

Moving beyond timeline recognition, this section provides an explicit migration playbook for IAM systems, addressing identity providers, HSMs, code signing, and device credentials.

POST-QUANTUM CRYPTOGRAPHY MIGRATION TIMELINE FOR IAM



Track 1: Identity Provider Migration

- 2025: Cryptographic inventory of all identity assertion signing (SAML, OIDC, JWT)
- 2026-27: Pilot hybrid certificates (classical + ML-KEM) in non-production environments
- 2028-30: Production migration to FIPS 203/204 compliant signing for all identity tokens

Track 2: HSM & Key Management

- 2025: Inventory all HSM-protected keys (credential vaults, certificate authorities, MFA seeds)
- 2026-28: Deploy PQC-ready HSMs in hybrid mode (dual algorithm support)
- 2029-31: Full PQC migration for all key material with escrow and recovery procedures

Track 3: Code Signing & Certificates

- 2025-26: Audit all code-signing certificates in identity infrastructure (plugins, connectors, agents)
- 2027-29: Implement dual-signing (classical + ML-DSA) for all identity-related software
- 2030-32: Transition to PQC-only signing aligned with NIST deprecation schedule

Track 4: Device & IoT Credentials

- 2026-27: Assessment of all device certificates (SCADA, lab instruments, manufacturing controllers)
- 2028-31: Phased migration of device identity certificates to PQC-compatible algorithms
- 2032-35: Complete migration ensuring all GxP device identities are quantum-resistant

CRITICAL: 20+ YEAR RETENTION

GxP documents with 20+ year retention requirements signed today must use cryptographic algorithms that remain verifiable in 2046 and beyond. Organizations must implement crypto-agility NOW to ensure audit trail integrity throughout regulatory retention periods.

17. Conclusion: Identity as Competitive Advantage

The evidence from global implementations is unequivocal: identity represents not merely a security cost center, but a foundational GxP infrastructure investment that underpins regulatory compliance, operational resilience, and strategic competitive advantage.

THE STRATEGIC IMPERATIVE

Organizations that establish robust identity governance frameworks today will emerge as industry leaders. Those that delay face escalating regulatory risk, competitive disadvantage, and potential personal liability for board members under evolving EU legislation. The Identity Utility Paradigm provides the blueprint—the implementation is yours to execute.

Key takeaways for board-level decision makers:

- Investment: Multi-year capital programme with demonstrated 127% IRR and 8.2-month payback (Appendix C)
- Proven ROI: 85% faster provisioning, 73% cost reduction, 50-75% audit time reduction across 40+ enterprises
- Regulatory: 21 CFR Part 11, Annex 11, DORA, NIS2, EU AI Act, ISO 42001 — combined penalty up to 7% turnover
- Framework: IUMM provides structured progression with self-assessment tooling (Appendix D)
- Timeline: EU AI Act high-risk effective Aug 2026; DORA already in force; PQC deprecation 2030
- AI Governance: Worked ITDR examples and RACI matrix ready for ISO 42001 conformity (Section 15)
- Competitive edge: Mature identity infrastructure enables 2-3x faster M&A; integration and cloud adoption

This whitepaper provides the blueprint. The implementation is yours to execute.

APPENDIX A: Board Briefing Insert & Capital Plan

BOARD BRIEFING: IDENTITY UTILITY INVESTMENT DECISION

Purpose: This 2-page insert is designed for direct inclusion in board packs. It presents the identity utility investment decision with explicit trade-offs, a 12-18 month capital plan scenario, and sensitivity analysis for delayed implementation.

Decision Required

Approve a 3-year capital investment programme of $2.55M to transform identity infrastructure from fragmented IT service (IUMM Level 2) to validated GxP utility (IUMM Level 4), with staged deployment delivering measurable returns from Month 6.

Capital Plan: 18-Month Scenario

Period	CapEx	OpEx	Cumulative	Expected Benefit
Months 1-6 (Foundation)	$450K	$85K/yr	($535K)	Baseline established; assessment complete
Months 7-12 (Core Infra)	$280K	$120K/yr	($935K)	IGA + MFA live; $420K FTE savings begin
Months 13-18 (Advanced)	$170K	$145K/yr	($1.25M)	PAM + ITDR live; full $1.24M benefit run-rate
Year 2	$50K	$165K/yr	($1.46M)	Optimisation; NPV positive from Month 14
Year 3	$30K	$175K/yr	($1.67M)	Level 4 achieved; 3-year NPV: $2.1M

Sensitivity Analysis: Cost of Delay

Delay Scenario	Additional Risk Exposure	Foregone Benefit	Total Cost of Delay
6-month delay	$255K (probability-weighted regulatory fine)	$620K (6 months of foregone savings)	$875K
12-month delay	$510K (includes EU AI Act exposure from Aug 2026)	$1.24M (full year of foregone savings)	$1.75M
18-month delay	$765K (DORA + EU AI Act cumulative exposure)	$1.86M (18 months of foregone savings)	$2.63M

Trade-Offs for Board Discussion:

• Build vs. Buy: Managed Identity Service (IDaaS) reduces Year 1 CapEx by 40% but increases 5-year TCO by 15%

• Phased vs. Big-Bang: Phased approach (recommended) delivers value from Month 6 but extends full deployment to Month 30

• Single-vendor vs. Best-of-breed: Single vendor reduces integration cost by 25% but creates concentration risk

• Internal vs. External resource: Big 4 advisory accelerates Phase 1 by 8 weeks but adds $180K-$250K

APPENDIX B: CXO/CTO Architecture Annex

Product-specific mapping of the Identity Utility Reference Architecture for technical decision-makers.

Identity Provider Layer: Product-Agnostic Design Choices

Capability	Microsoft Entra ID	Okta	Ping Identity	Selection Criteria
SSO Protocol	SAML 2.0, OIDC, WS-Fed	SAML 2.0, OIDC	SAML 2.0, OIDC, WS-Fed	Prefer OIDC for new integrations
MFA Options	FIDO2, Push, OTP, Cert-based	FIDO2, Push, OTP, Biometric	FIDO2, Push, OTP	FIDO2 as target; OTP for legacy
Conditional Access	Risk-based policies, device compliance	Adaptive MFA, behavioural	Risk-based, step-up auth	Context-aware risk scoring
GxP Validation	SOC 2, ISO 27001, FedRAMP	SOC 2, ISO 27001	SOC 2, ISO 27001, FedRAMP	Require SOC 2 Type II minimum
Sovereign Cloud	EU Data Boundary, Gov regions	Cell-based arch	Regional deploy	Match data residency requirements

IGA Layer: Governance Platform Comparison

Capability	SailPoint	Saviynt	Selection Criteria
Provisioning	300+ connectors, low-code workflows	200+ connectors, cloud-native	Connector coverage for GxP systems
Certification	Risk-weighted, AI-recommended	Risk-based, micro-certifications	Risk-weighted review prioritisation
SoD	Pre-built SoD matrix, cross-application	Real-time SoD with fine-grained	Cross-application SoD enforcement
AI/ML	AI-recommended access, outlier detection	AI analytics, risk quantification	Explainable AI for GxP audit trail

PAM Layer

- CyberArk: Market leader for credential vaulting and session recording; strongest GxP validation story
- Delinea: Cloud-native PAM with simplified deployment; faster time-to-value for greenfield environments
- Saviynt: Converged IGA+PAM in single platform; reduces integration complexity but less deep PAM capability

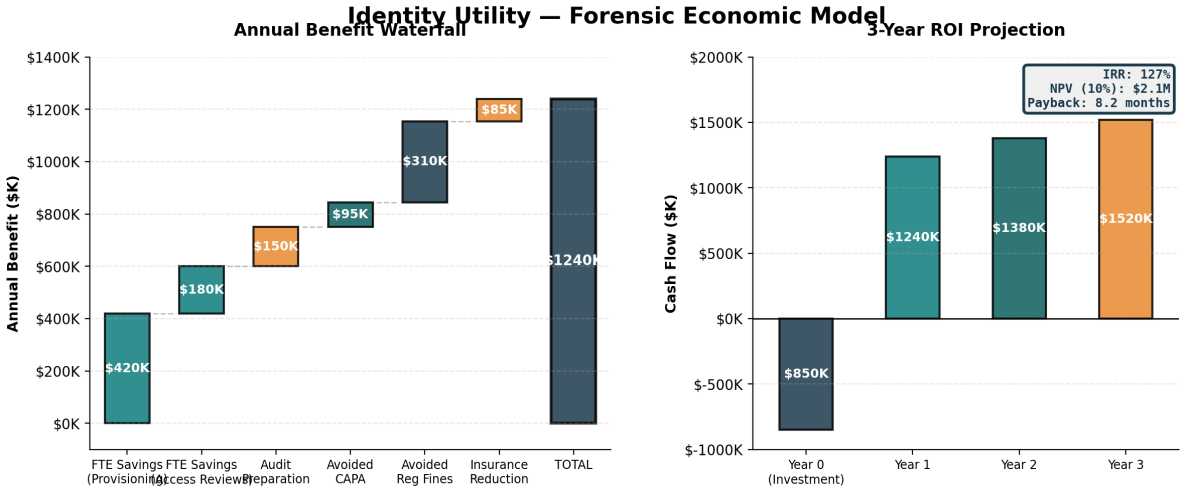
ZTNA Layer

- Zscaler ZPA: Application-level micro-segmentation; strongest enterprise scale and regulatory compliance
- Netskope Private Access: Inline security with CASB integration; best for multi-cloud environments
- Microsoft Entra Private Access: Native Azure integration; lowest friction for Microsoft-centric estates

APPENDIX C: Forensic Economic Model & Business Case Template

This worked model ties the headline metrics (85%/73%/6-month payback) to granular operational drivers. Use as a template for your organisation's specific parameters.

IDENTITY UTILITY: FORENSIC ECONOMIC MODEL



Benefit Decomposition (Annual, Steady-State)

Benefit Category	Driver	Calculation	Annual Value
FTE Savings: Provisioning	12 FTEs × 85% time saved on JML events	12 × $85K × 0.85 × 0.49 (provisioning share)	$420K
FTE Savings: Access Reviews	8 FTEs × 73% faster certification cycles	8 × $85K × 0.73 × 0.36 (review share)	$180K
Audit Preparation	6 weeks → 48 hours × 3 audits/year	3 × 5 consultant-weeks × $6K/week	$150K
Avoided CAPA	8 identity-related deviations/year → 0	8 × $12K average CAPA cost	$96K
Regulatory Fine Avoidance	Probability-weighted: 15% × $2.1M exposure	0.15 × $2.1M =	$310K
Insurance Premium	Cyber insurance discount for mature IAM	$1.7M premium × 5% reduction	$85K
TOTAL			**$1.24M / year**

Investment Summary & Returns

Metric	Value	Note

Total 3-Year Investment	$2.55M	CapEx $980K + OpEx $1.57M
Annual Benefit (steady-state)	$1.24M	Fully realised from Month 18
Payback Period	8.2 months	From first benefit realisation
Internal Rate of Return	127%	3-year calculation
Net Present Value (10%)	$2.1M	3-year discounted cash flow
Benefit-to-Cost Ratio	2.46x	Over 3-year programme

APPENDIX D: IUMM Self-Assessment Questionnaire

Complete this questionnaire with your CISO and identity team in approximately 60 minutes. Score each dimension 1-5 using the criteria below. Your aggregate score determines IUMM level.

IDENTITY UTILITY MATURITY MODEL: 60-MINUTE SELF-ASSESSMENT

A. GOVERNANCE	Score (1-5)
Is identity formally classified as GxP infrastructure?	____
Is there single executive accountability for identity across all BUs?	____
Does the board receive regular identity KPI reporting?	____
Is identity investment governed through capital planning?	____

B. PROVISIONING	Score (1-5)
Is provisioning automated via HR authoritative source?	____
What is average time from hire to full system access?	____
Are deprovisioning actions automated on termination?	____
Is there automated detection of orphaned/dormant accounts?	____

C. AUTHENTICATION	Score (1-5)
What percentage of GxP applications use SSO?	____
Is MFA deployed across all GxP systems (including legacy)?	____
Are phishing-resistant methods (FIDO2) in use or planned?	____
Is authentication risk-adaptive (context-aware)?	____

D. PRIVILEGED ACCESS	Score (1-5)
Are all privileged credentials stored in a vault?	____
Is standing privileged access eliminated (JIT model)?	____
Are privileged sessions recorded for forensic audit?	____
Are third-party privileged sessions time-bounded?	____

E. COMPLIANCE	Score (1-5)
Can you produce audit evidence for any framework in < 48 hours?	____
Are compliance reports automated (not manually compiled)?	____
Is identity infrastructure validated per GAMP 5?	____
Do you maintain a complete non-human identity inventory?	____

F. THREAT DETECTION	Score (1-5)

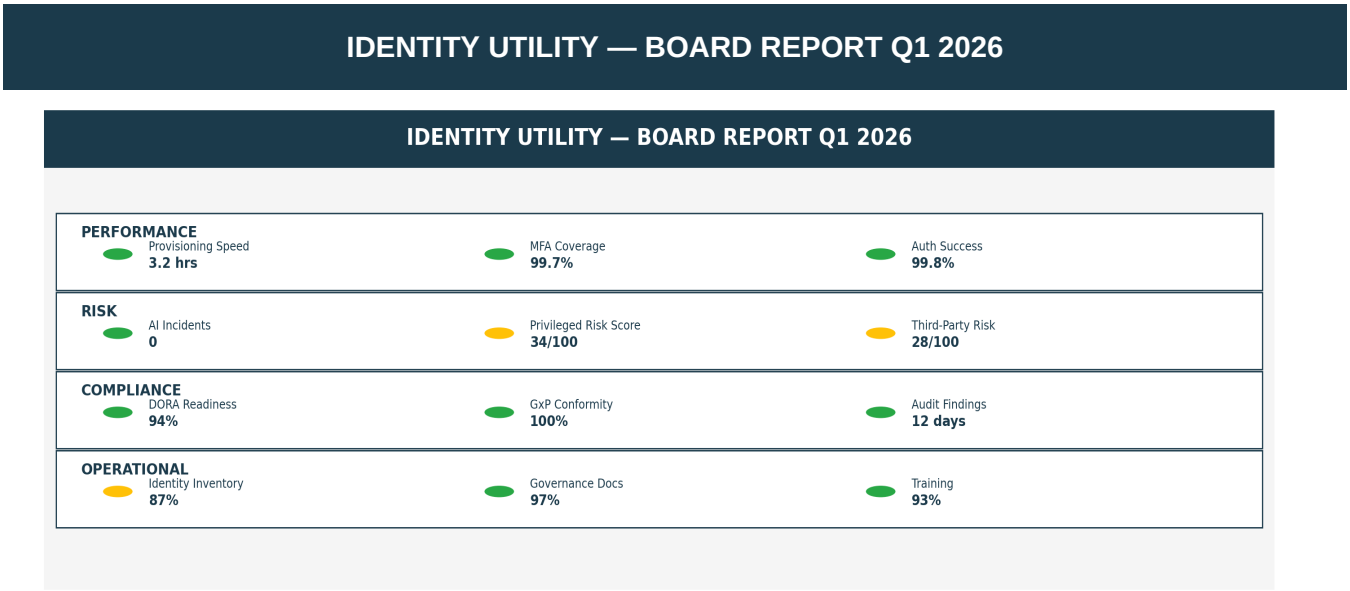
Is behavioural analytics deployed on identity events?	____
Are automated response playbooks active for identity threats?	____
Is there unified monitoring across human and machine identities?	____
Can you produce forensic identity timelines for investigations?	____

Scoring Guide:

Score	IUMM Level	Interpretation
24-48	Level 1: Ad Hoc	Significant gaps; immediate action required
49-72	Level 2: Managed	Basic controls in place; systematic improvement needed
73-96	Level 3: Defined	Solid foundation; ready for advanced capability deployment
97-108	Level 4: Optimized	Mature infrastructure; focus on AI and continuous improvement
109-120	Level 5: Strategic Utility	Industry-leading; identity as competitive advantage

APPENDIX E: Sample Board RAG Report

This one-page dashboard is designed for direct inclusion in quarterly board reporting packs. Red/Amber/Green indicators with concise commentary enable non-technical board members to assess identity infrastructure health at a glance.



Commentary for Board Discussion:

- **GREEN — Provisioning Speed (3.2 hrs):** Exceeds 4-hour target; driven by automated HR-to-IGA integration deployed in Month 8. 85% improvement vs. pre-programme baseline of 5.2 days.
- **AMBER — Privileged Risk Score (34/100):** Above 30 target due to 12 legacy manufacturing systems still requiring standing privileged access. Remediation: CyberArk JIT deployment scheduled Q2 2026; expected to reduce score to 22.
- **AMBER — Identity Inventory (87%):** Below 100% target; gap is in non-human identities for 3 recently acquired facilities. Remediation: IoT/OT identity discovery scan scheduled March 2026.
- **GREEN — GxP Conformity (100%):** All identity systems validated per GAMP 5 with current qualification documentation. Next periodic review: June 2026.
- **Escalation Item:** EU AI Act high-risk obligations effective August 2026. Section 15 RACI matrix approved; ISO 42001 gap assessment in progress (completion target: April 2026).

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

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

Mr. Upadrasta has worked with the largest corporations worldwide to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, SAS70, DORA, NIS2, and the EU AI Act. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, AI governance (ISO 42001), M&A; cyber due diligence, and board reporting for identity and cyber risk.

Professional Memberships & Academic Positions

- 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, (ISC)² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Areas of Expertise

- Identity & Access Management (IAM) | Privileged Access Management (PAM) | Zero Trust Architecture
- DORA Compliance | NIS2 | EU AI Act | ISO 42001 AI Governance | Board Reporting
- M&A Cyber Due Diligence | GxP Compliance (21 CFR Part 11, EU GMP Annex 11)
- Post-Quantum Cryptography | Identity Fabric Architecture | NIST SP 800-63

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

References

Primary Regulatory Sources

1. FDA 21 CFR Part 11, Electronic Records; Electronic Signatures

2. EU GMP Annex 11 (Revised), Computerised Systems

3. MHRA GxP Data Integrity Guidance, March 2018

4. DORA Regulation (EU) 2022/2554, EUR-Lex

5. NIS2 Directive (EU) 2022/2555, EUR-Lex

6. EU AI Act Regulation (EU) 2024/1689, EUR-Lex

7. ICH Q10, Pharmaceutical Quality System

8. PIC/S PI 041-1, Good Practices for Data Management

9. WHO Technical Report Series 1033

Standards and Frameworks

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

11. NIST SP 800-207, Zero Trust Architecture

12. NIST SP 800-63-4, Digital Identity Guidelines (2025)

13. NIST AI Risk Management Framework (AI RMF 1.0)

14. ISPE GAMP 5, Risk-Based Approach to GxP Computerized Systems

15. NIST FIPS 203/204/205, Post-Quantum Cryptography Standards (2024)

16. CISA/NACD Director's Handbook on Cyber-Risk Oversight (2025)

17. W3C Decentralized Identifiers (DIDs) v1.0

18. W3C Verifiable Credentials Data Model 2.0

Industry Research

19. NACD Board AI Governance Framework 2025

20. Gartner Identity Fabric Reference Architecture 2025

21. KuppingerCole Identity & Access Management Reference Architecture 2025

22. IBM Cost of a Data Breach Report 2025

23. Verizon Data Breach Investigations Report 2025

24. Gartner Legal Technology Market Analysis 2025-2026

Technology Documentation

25. Microsoft Entra ID Architecture Guides

26. Microsoft Azure Confidential Computing Documentation

27. SailPoint Identity Governance Documentation

28. CyberArk Privileged Access Management Documentation

29. Okta Identity Engine Documentation

30. Zscaler Zero Trust Exchange Architecture