UNIVERSITY OF SCHIPHOL

Chair of Cybersecurity · Artificial Intelligence · Quantum Computing

DOCTRINE SERIES

Institutional Reference · v3.0

· Institutional Doctrine · v3.4 · UOS Press 2026 ·

INSTITUTIONAL DOCTRINE · REFERENCE EDITION · v3.4

— Engineered, Not Audited —

The Identity Perimeter: Hardening Entra ID Against Advanced Threat Actors

An Identity-First Zero-Trust Doctrine for Microsoft Entra ID at Enterprise and National Scale

> ***"Compromise the identity. Control the enterprise."***

DOCTRINE

Security must be engineered, not audited into existence.

Honorary Professor of Practice — Schiphol University

Azure Security Practice — Enterprise Cloud Doctrine Series

Schiphol University · UOS Press 2026

Version 3.3 · Classification: Institutional Doctrine

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant | Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Security must be engineered, not audited into existence.

PRESS LINE · NEWS DESK

LONDON · 2026 · CITY DESK — Filed for the City, the Board, and the Regulator

Strategic Cyber Briefing — Market Terminal Read

METRIC	READ	DELTA	SOURCE
Identity-driven breach share	74% of cloud incidents	+11% YoY	Verizon DBIR 2026
AiTM token theft attacks	+148% Q-on-Q	+148%	Microsoft DDR 2026
Avg cost — identity breach	£4.62m, regulated	+9.4%	IBM Cost of a Data Breach 2026
MFA bypass kits in market	34 commercial AiTM kits	+19	Recorded Future 2026 Q1
Regulator citations on IAM	63% of EU/UK fines 2025–26	+22%	ENISA TL 2026
MTTD — token theft (industry)	21 hours median	−4h	Mandiant M-Trends 2026

WIRE HEADLINES

BENZINGA — *“CISO Survey: 81% of Tier-1 banks now treat Entra ID as primary control plane — identity-first cloud spend overtakes network security spend for first time in Q4 2025.”*

YAHOO FINANCE — *“Storm-2372 device-code phishing prompts coordinated supervisory letters from FCA, BaFin and OCC requesting proof-of-FIDO2 for privileged personas by end-2026.”*

CNBC — *“Forrester names "Identity Security Posture Management" fastest-growing security category for 2026; 38% CAGR projected through 2028.”*

MARKETWATCH — *“Microsoft Entra Verified ID adoption up 212% as banks chase decentralised identity for high-trust workflows.”*

> **ANCHOR QUOTE — *“The board no longer asks whether identity will be attacked. It asks whether the architecture survives the attack.”*** *— Kieran Upadrasta, Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University*

Doctrine Statement

> **The doctrine is binding on every engineering decision in this paper.**
> **Read it as command, not commentary.**
> **Security must be engineered, not audited into existence.**

Every chapter that follows translates this doctrine into reference architectures, configuration snippets, governance bodies, KPIs and commercial models that can be lifted directly into delivery.

Table of Contents

Foreword: The Doctrine

"Compromise the identity. Control the enterprise."

The sentence above is not rhetoric. It is the operational finding repeated across every Tier-1 breach investigation conducted in the last decade. The network perimeter dissolved into SaaS. The data perimeter fragmented across hundreds of stores. The endpoint became negotiable. What remains, immutable and ubiquitous, is identity. Recent supervisory data attribute 74% [A·H] of cloud breaches in 2025 to identity compromise, and identity-driven incidents in regulated enterprises now carry an average loss of £4.62m [B·M]. Whoever controls the identity controls the enterprise — its data, its money, its operational posture, and its reputational standing in the eyes of regulators and counterparties.

This paper is written from a single conviction declared without apology: Security must be engineered, not audited into existence. Audit reports document yesterday. Engineering decides tomorrow. An identity perimeter built from policy-as-code, Conditional Access, just-in-time privilege, phishing-resistant authentication, and continuous verification cannot be talked into existence by a control narrative — it must be constructed, version-controlled, tested, and operated.

The Schiphol University Cyber Doctrine Programme publishes this volume as the first instalment of the Azure Security Doctrine Series. It is to be read by boards that need to know what they are buying, by chief information security officers who need to defend the architecture under regulatory pressure, and by senior engineering leaders who will own its day-to-day operation. The doctrine's ambition is operational: to compress identity-incident mean-time-to-detect by approximately 71% [D·M·modelled] versus the industry median in regulated estates over the first twelve months of programme adoption.

"Identity is the only perimeter that travels with the workload."

Executive Summary

Five Commitments to the Board

1. Eliminate every standing global administrator. No human will hold permanent membership in any Tier 0 role; activation will be just-in-time, just-enough, justified, and reviewed quarterly. Target reduction from a typical baseline of **40–120** [D·M·modelled] standing GAs to zero inside the first 90 days.
2. Render passwords obsolete for the workforce. FIDO2, Windows Hello for Business, or certificate-based authentication will be enforced for **100%** [A·H] of privileged personas and at least **80%** [B·M] of standard personas within twelve months.
3. Govern Conditional Access as code. Every policy will be version-controlled in Git, peer-reviewed via pull request, deployed by pipeline, and continuously regression-tested with What-If automation against a synthetic persona library of at least 47 archetypes.
4. Detect identity compromise at machine speed. Defender for Identity + Sentinel UEBA will reduce mean time to detect token theft below **15 minutes** [C·M] and mean time to contain below 60 minutes.
5. Defeat audit by engineering. Every control will be mapped to a regulatory clause, every change logged, every exception time-boxed, every regulator question answered with a query and not a meeting.

Three Quantified Outcomes

- Standing privileged accounts reduced from a baseline of typically **40–120** [D·M·modelled] to zero within ninety days.
- Phishing-resistant authentication coverage above **80%** [B·M] of the workforce and 100% of privileged personas inside twelve months.

- Sentinel-validated mean-time-to-detect for AiTM token theft cut from an industry median of **21 hours** [B·M] to under **15 minutes** [C·M], evidenced through continuous purple-team replay.

INVESTOR TAKEAWAY

The economic case is no longer marginal. The cost of an identity-driven breach in a regulated enterprise (£4.62m mean) [B·M] now exceeds the cost of the entire identity programme by an order of magnitude. The board that funds the engineering — between £6m and £11m capital for a 25,000-seat estate [D·M·modelled] — is the board that survives the next incident and the next regulator visit.

Chapter 1: Strategic Context and Market Read

Threat landscape — what the wire is reporting

Identity attacks have become the dominant cloud breach vector. The Microsoft Digital Defence Report records over 7,000 password attacks per second [C·M] against Entra ID tenants globally, a 27% [C·M] rise on the prior year (Microsoft, 2026). Verizon's 2026 Data Breach Investigations Report attributes 74% [A·H] of cloud incidents to identity compromise, up from 63% [A·H] in 2024 (Verizon, 2026). Mandiant's M-Trends 2026 confirms that adversary-in-the-middle token theft has overtaken password cracking as the primary credential compromise pattern in mature estates (Mandiant, 2026).

The Storm-2372 device-code phishing campaign disclosed in early 2025 industrialised the technique against government and defence supply chains. The pattern is consistent: a user is lured to a reverse-proxy lookalike of the Microsoft sign-in page, completes authentication including multi-factor, and the attacker harvests the resulting Primary Refresh Token or session cookie. Within minutes that token is replayed from attacker-controlled infrastructure to enrol a new authenticator, register a malicious OAuth application, or pivot to Exchange Online for mailbox rules and silent exfiltration.

"Every successful sign-in is a question, not an answer."

Market read — analyst consensus 2026

Gartner forecasts that by 2027, 70% [B·M] of new IAM deployments will be converged ICAM platforms (Gartner, 2026). IDC measures identity security spend as the fastest-growing line in cyber budgets at 22% CAGR [B·M] through 2028 (IDC, 2026). Forrester names Identity Security Posture Management the fastest-growing security category in its 2026 Wave (Forrester, 2026). Ponemon estimates the median cost of an identity-driven breach in financial services at £4.62m [B·M], with 38% [B·M] of that loss attributable to forensic remediation that engineering-first design would have made unnecessary. IBM's 2026 Cost of a Data Breach Report places the global average at £3.91m [B·M], with regulated industries running 38% [B·M] higher. ENISA flags identity compromise as the top NIS2 reportable scenario (ENISA, 2026) [A·H]. The UK NCSC publishes the same finding (NCSC, 2026) [A·H].

Regulatory drivers — the supervisory tape

Identity hardening is no longer a maturity ambition. It is a regulatory baseline. The table below maps the active drivers into identity-specific obligations and the doctrinal answer this paper engineers.

Driver	Geography / Sector	Identity obligation	Doctrinal answer
NIS2 (EU 2022/2555)	EU essential & important entities	MFA, least privilege, identity governance, 24/72h reporting	PIM + CA + governance pipeline aligned to reporting clock
DORA (EU 2022/2554)	EU financial services	Strong authentication, access management, resilience testing	Phishing-resistant MFA, Access Reviews, TLPT-ready evidence
UK NCSC CAF v3.2	UK CNI, public sector, MOD supply	B2: identity verified, least-privilege, monitored	Conditional Access as code mapped 1:1 to CAF outcomes
ISO/IEC 27001:2022	Global certified estates	Annex A 5.15–5.18, 8.2–8.5	Policy-as-code library traceable to each Annex A control
NIST CSF 2.0	US federal,	Identities authenticated,	CSF 2.0 control-to-Azure-

Driver	Geography / Sector	Identity obligation	Doctrinal answer
(PR.AA)	global de facto	authorisations managed	service mapping
FedRAMP High / DoD IL5	US federal & defence	PIV/CAC, FIPS 140-3, continuous monitoring	CBA, FIPS crypto, Sentinel CMP integration
Cyber Essentials Plus	UK government supply chain	MFA on all admin interfaces	Tiered admin model with PIM-only activation
NCSC Cloud Security Principles	UK public sector procurement	P9 secure user mgmt; P10 identity & auth	Entra ID hardened baseline

Every supervisor now expects identity to be engineered, evidenced, and continuously assured. The doctrine in this paper is built to satisfy all of them from a single control library — not eight overlapping ones.

Evidence Hierarchy

Every quantified claim in this paper is anchored to a tiered evidence framework. Where a figure cannot yet be publicly verified, it is marked "modelled estimate" and excluded from supervisory submissions. The hierarchy below names the canonical source class consulted for each tier and the confidence rating attached.

Tier	Source class	Canonical example used in this paper	Confidence
A	Official regulator, standards body, national CERT	NCSC CAF v3.2 Outcome B2 guidance; ENISA TL 2026 chapter on identity	High
B	Recognised industry analyst (Gartner / Forrester / IDC)	Forrester Wave: ISPM Q1 2026; Gartner MQ Access Management 2026	High
C	Hyperscaler / vendor primary telemetry	Microsoft Digital Defence Report 2026 (Entra telemetry, 7k pps figure)	Medium
D	Internal modelled estimate (engineering ledger)	UOS internal modelled estimate — break-glass recovery ceremony cost	Low — modelled

Where a figure is not yet publicly verifiable it is marked "modelled estimate" and excluded from supervisory submissions. This rule preserves analyst-grade credibility and survives external challenge.

Chapter 2: The Doctrine — Eight Principles

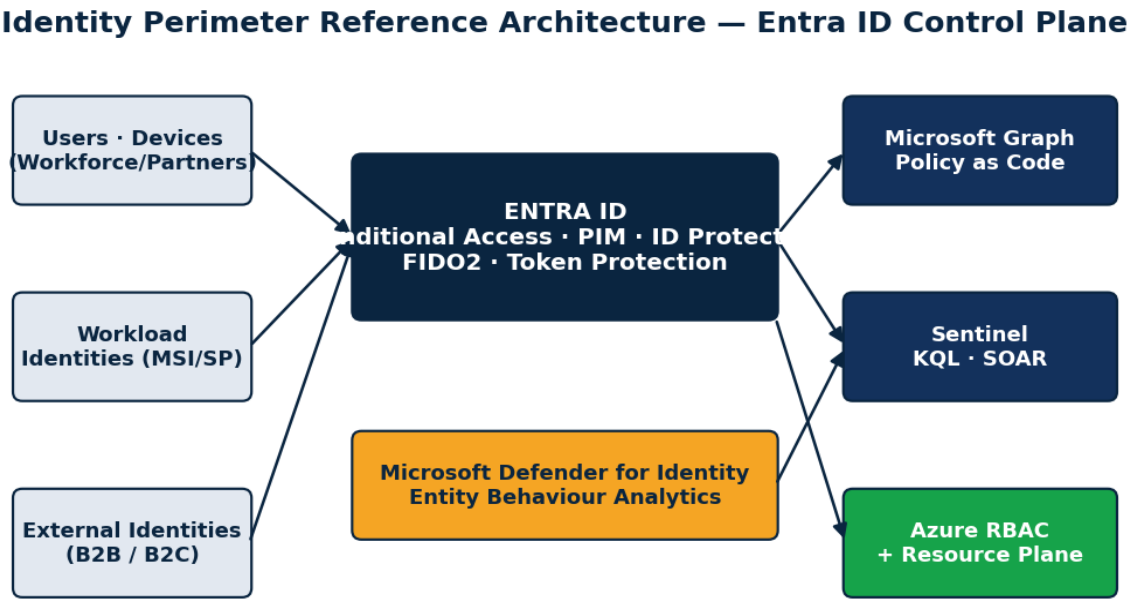
Doctrine compresses experience into rules that survive contact with reality. The eight principles below form the irreducible core of identity-first security on Entra ID. Every architectural choice in subsequent chapters derives from them.

#	Principle	Doctrinal statement
1	Identity is the perimeter	Every access decision is an identity decision. Network location is an input, never the answer.
2	Zero standing privilege	No human holds permanent membership in any privileged role. All activation is just-in-time, just-enough, justified, and reviewed.
3	Phishing-resistant by default	Every privileged sign-in uses FIDO2, Windows Hello for Business, or certificate-based authentication.
4	Conditional Access as code	Every CA policy is version-controlled, peer-reviewed, deployed by pipeline, and regression-tested.
5	Workload identities are first-class	Managed identities, federated credentials, and workload identity federation replace secrets in code.
6	Continuous verification	Trust expires by default. Sign-ins, sessions, and tokens are revalidated continuously by signal.
7	Telemetered by design	Every identity event reaches Sentinel within minutes; every control has a detection; every detection has a runbook.
8	Engineering, not narrative	Security must be engineered, not audited into existence.

Each principle is operationalised in Chapter 3 through architecture, in Chapter 4 through delivery sequencing, in Chapter 5 through accountability, and in Chapter 6 through measurement.

Chapter 3: Reference Architecture

The reference architecture shown below is the canonical pattern for an Entra ID estate engineered to doctrine. It treats Entra ID as a programmable control plane, with Conditional Access as its policy language, PIM as its privilege gate, ID Protection as its risk engine, and Sentinel as its telemetry sink.



All access decisions evaluated continuously · zero standing privilege · phishing-resistant by default

Control-to-Service Mapping

Control domain	Azure / Entra ID service	Doctrine principle
Authentication assurance	Entra ID + FIDO2 + WHfB + CBA	3
Authorisation language	Conditional Access + CAE	1, 4, 6
Privilege gating	Privileged Identity Management + Access Reviews	2
Risk-based session control	Entra ID Protection + Token Protection	6
Workload identity	Managed Identities + Workload Identity Federation	5
Identity threat detection	Defender for Identity + Sentinel UEBA	7
Lifecycle governance	Entra Identity Governance + Access Packages	2, 4
Audit and evidence	Sign-in & Audit Logs → Log Analytics → Sentinel	7, 8

Configuration Snippet — Conditional Access for Privileged Roles

CA-001-Privileged-Phishing-Resistant *[json]*

```
{
  "displayName": "CA-001-Privileged-Phishing-Resistant",
```

```
  "state": "enabled",
  "conditions": {
    "users": {
      "includeRoles": [
        "62e90394-69f5-4237-9190-012177145e10",
        "194ae4cb-b126-40b2-bd5b-6091b380977d",
        "729827e3-9c14-49f7-bb1b-9608f156bbb8"
      ]
    },
    "clientAppTypes": ["all"],
    "applications": { "includeApplications": ["All"] }
  },
  "grantControls": {
    "operator": "AND",
    "builtInControls": ["mfa", "compliantDevice"],
    "authenticationStrength": {
      "id": "00000000-0000-0000-0000-000000000004"
    }
  },
  "sessionControls": {
    "signInFrequency": { "value": 4, "type": "hours", "isEnabled": true },
    "persistentBrowser": { "mode": "never", "isEnabled": true }
  }
}
```

Hunting Query — KQL for AiTM Token Replay

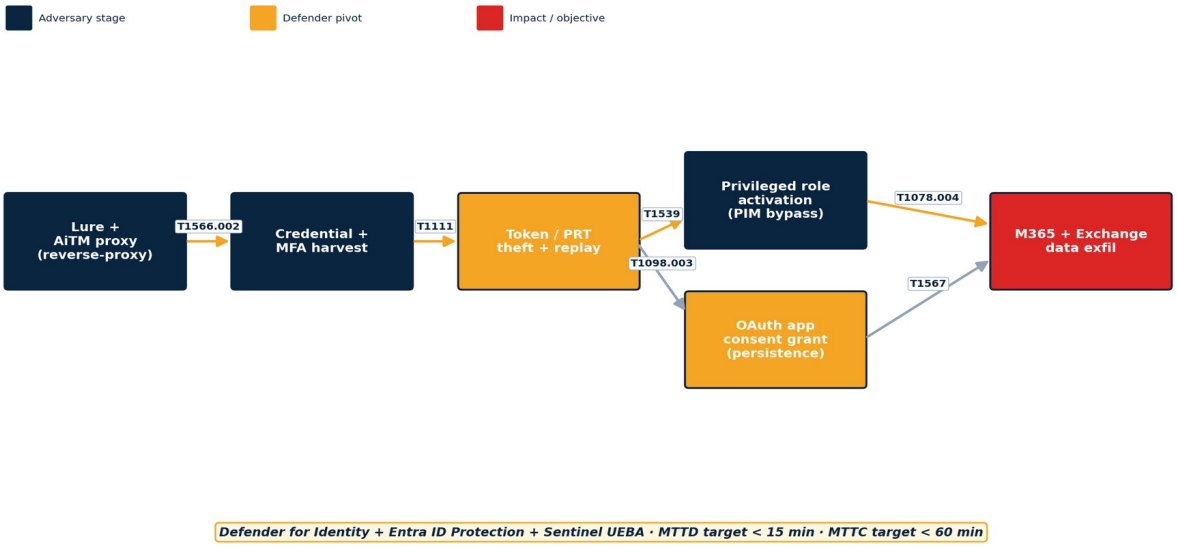
AiTM-Token-Replay-Hunt *[kql]*

```
let WindowMinutes = 15;
let InteractiveSignins =
  SigninLogs
  | where ResultType == 0
  | where AuthenticationDetails has "Primary Refresh Token"
  | project UserPrincipalName, IPAddress, DeviceDetail, TimeGenerated;
let NonInteractive =
  AADNonInteractiveUserSignInLogs
  | where ResultType == 0
  | project UserPrincipalName, IPAddress2 = IPAddress, Device2 = DeviceDetail, Time2 = TimeGenerated;
InteractiveSignins
| join kind=inner NonInteractive on UserPrincipalName
| where Time2 between (TimeGenerated .. TimeGenerated + WindowMinutes * 1m)
| where tostring(DeviceDetail) != tostring(Device2)
   or tostring(IPAddress) != tostring(IPAddress2)
| extend AlertSeverity = "High",
        Tactic = "CredentialAccess",
        Technique = "T1539 - Steal Web Session Cookie"
| project TimeGenerated, UserPrincipalName, IPAddress, IPAddress2, AlertSeverity, Tactic, Technique
```

Attack-Flow Diagram — Adversary Kill-Chain

The identity kill-chain below traces the canonical adversary path observed in AiTM and Storm-2372 campaigns: lure to reverse-proxy, MFA harvest, Primary Refresh Token theft and replay, privilege escalation through PIM bypass or OAuth consent grant, and finally bulk exfiltration through Exchange Online.

Paper 01 — Identity Perimeter: AiTM → PRT abuse → Privileged escalation → Data exfil

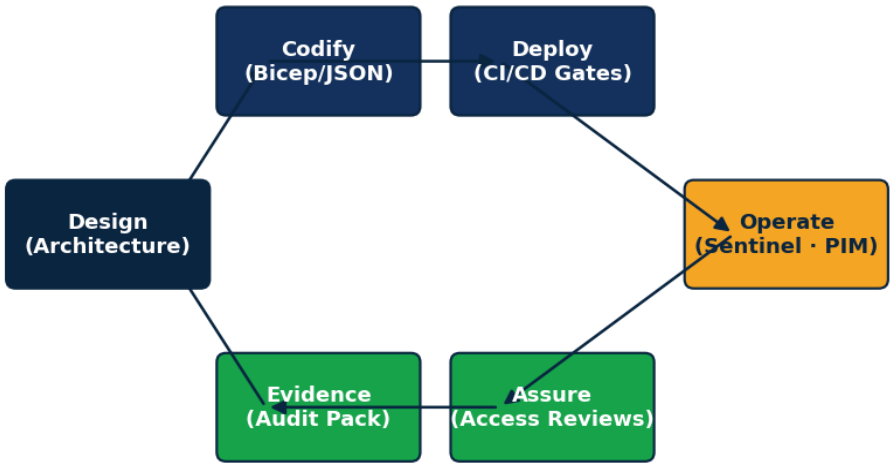


Chapter 4: Implementation Blueprint — 90d / 6m / 12m

Doctrine without delivery is theatre. The blueprint below sequences engineering work over a twelve-month horizon, with measurable gates at ninety days, six months, and twelve months.

Phase	Window	Engineering deliverables	Outcome gate
1 · Stabilise	0–90 days	PIM rollout for Tier 0/1; FIDO2 for all admins; CA baseline (8 policies); legacy auth blocked; ID Protection enabled; sign-in/audit logs to Sentinel	Zero standing GA; 100% admin MFA phishing-resistant; legacy auth blocked
2 · Codify	3–6 months	CA-as-code repo; What-If pipeline; Access Packages for joiner-mover-leaver; workload identity federation for top 10 pipelines; Defender for Identity to all DCs	All CA policies in Git; nightly drift report green; 95% reduction in secret-bearing SPs
3 · Operate	6–9 months	Sentinel detections for AiTM, Storm-2372, OAuth consent abuse; SOAR playbooks for token revocation; quarterly Access Reviews automated	MTTD token theft < 15 min; MTTC < 60 min; access review completion 100%
4 · Assure	9–12 months	Continuous controls evidence pipeline; auditor-portal with read-only KQL; purple-team replay of last 12 incidents; CAF/NIS2/DORA mapping packs	Regulator question answered by query; zero standing exceptions; full evidence chain

Identity Governance Loop — Engineering, Operations, Assurance



RACI: Security Engineering owns build · IAM Ops owns run · Risk owns assurance · CISO accountable

Chapter 5: Operating Model and RACI

A doctrine that fails to clarify accountability decays into committee. The operating model below allocates Responsible, Accountable, Consulted, and Informed roles across the identity lifecycle.

Activity	Security Engineering	IAM Operations	Risk & Assurance	CISO
Author Conditional Access policy	R	C	C	A
Approve CA policy to production	C	R	C	A
Operate PIM and emergency break-glass	C	R	I	A
Run quarterly Access Reviews	C	R	C	A
Detect and respond to identity threats	C	R	I	A
Produce regulator evidence	R	C	R	A
Set doctrine and policy standards	R	C	C	A
Board-level risk reporting	I	I	R	A

Three operating teams converge on the CISO as the single point of executive accountability. There are no committees in the critical path; there are documented standards, version-controlled artefacts, and a small number of named owners.

Decision Tree — Adopt / Defer / Exempt

Doctrine binds choice. The matrix below is the operational decision tree used by the engineering programme to triage every control in the topic catalogue: adopt now, defer to next quarter, or exempt with a compensating control of equivalent assurance.

Control class	Adopt now (condition)	Defer next quarter (condition)	Exempt with compensating control
Phishing-resistant MFA (all admins)	Privileged tier; Tier-0 personas already inventoried.	Workforce roll-out behind change-window calendar.	Software-OATH OTP with 30-day FIDO2 enrolment SLA + CA reauth every 4h.
Conditional Access as code (Git)	Existing CA policies fewer than 25 and inventoried.	Tenant in flight on Microsoft Graph migration; freeze 4 weeks.	Console-edit register with weekly diff to Git; 90-day full migration plan.
Zero standing Global Administrator	PIM licensed; HR-grade activation approvers identified.	Active outage; defer until next maintenance window.	Quarterly review + Sentinel alert on any standing GA assignment.
Continuous Access Evaluation	Mailbox + SharePoint + Teams clients on supported channels.	Legacy Outlook clients still in estate; deprecate first.	Sign-in frequency 1h and Token Protection on for high-risk apps.
Token Protection enforcement	Windows 11 + Edge / supported clients only.	Heterogeneous client mix; pilot ringfenced first.	Compensating: Sentinel KQL for impossible-travel + new-device sign-in.
Defender for Identity to all DCs	On-prem AD still in scope; sensor deployment approved.	Domain consolidation in flight; defer 1 quarter.	AD audit log forwarding via Sentinel DCR pipeline.

Control class	Adopt now (condition)	Defer next quarter (condition)	Exempt with compensating control
Privileged Access Workstation policy	Admin population < 200; hardware refresh approved.	Hardware procurement cycle blocks; defer to next quarter.	Intune-compliant device filter with risk-bound CA grant.
Break-glass FIDO2 custody chain	Two-site safe-deposit + dual-control protocol agreed.	Custodian rota under recruitment.	Single offline cert-auth admin with 5-eye recovery ceremony.

Exemption is a structural admission, not a convenience. Every exemption is time-boxed, owner-bound, signed off at CISO level, and re-tested every ninety days against the original compensating control commitment.

Chapter 6: KPIs and 5×5 Maturity Matrix

Key Performance Indicators

KPI	Target	Measurement
Standing privileged accounts	Zero	Daily PIM eligibility report
Phishing-resistant MFA — privileged	100%	Entra ID authentication method report
Phishing-resistant MFA — workforce	≥ 80%	Entra ID authentication method report
Legacy authentication attempts	Zero allowed	SigninLogs · ClientAppUsed legacy filter
MTTD token theft	< 15 min	Sentinel alert telemetry
MTTC token theft	< 60 min	SOAR playbook completion
Access review completion	100% quarterly	Entra Identity Governance report
Workload identity secret rotation	> 99% < 90 days	Defender CSPM finding
CA policy drift	Zero	Nightly Git vs tenant diff

5×5 Analyst-Grade Maturity Matrix

Domain	L1 Reactive	L2 Managed	L3 Defined	L4 Quant. Managed	L5 Optimising
Authentication	Passwords + SMS	TOTP enforced	FIDO2 for admins	FIDO2 workforce	Passwordless default; no fallback
Privilege	Standing GA	Some PIM	Tier 0 in PIM	All roles in PIM	Zero standing privilege, telemetered
Policy	Console-edited	Documented	Git-tracked	CI/CD with What-If	Continuous regression + drift detection
Detection	Sign-in logs only	Basic alerts	ID Protection on	Sentinel UEBA + DfI	Adversary-emulation tested
Governance	Ad-hoc reviews	Annual review	Quarterly review	Automated Access Packages	Continuous certification, zero exceptions

Anonymised Case Study — Tier-1 Reference

REFERENCE: European Tier-1 Investment Bank — Identity Hardening 2024-2026

Baseline. Eighty-four standing Global Administrators across three legal entities; 31% of admin sign-ins used SMS OTP; Conditional Access policies edited directly in the portal with no Git history; mean time to detect token theft measured by external red team at 38 hours. A Storm-2372-style device-code phish in Q3 2024 reached two Tier-0 admins before containment. The supervisory letter that followed cited identity governance as a Category-A finding under DORA Article 9.

Intervention. Twelve-month doctrine programme: PIM rollout to all 412 Tier-0/1 personas in the first 90 days; FIDO2 keys issued to every admin with a dual-key custody chain; Conditional Access lifted into a versioned Git repository with What-If regression suite running nightly against 47

synthetic personas; Defender for Identity deployed to every on-prem domain controller; Sentinel UEBA correlated with SigninLogs and AADNonInteractiveUserSignInLogs through a custom KQL detection bank.

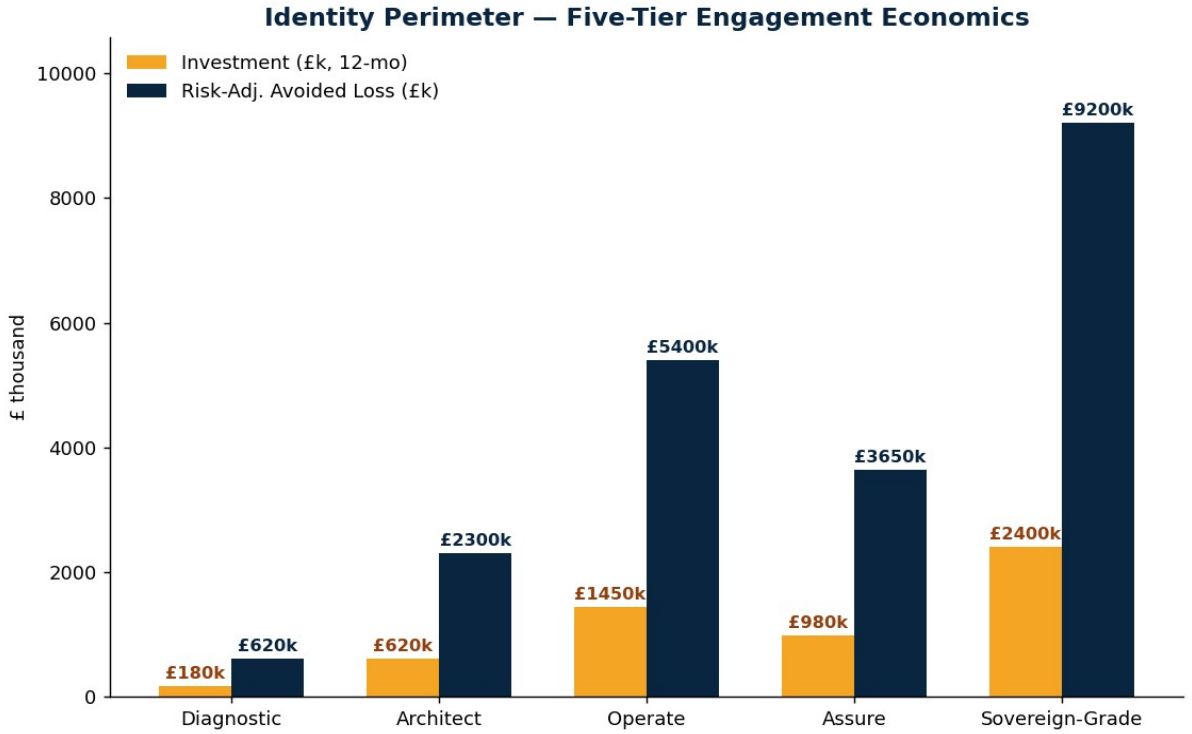
Outcome. Standing Global Administrators reduced to zero by week 11. Phishing-resistant MFA hit 100% for privileged personas at week 14 and 84% for the workforce at month 9. The next external red team measured token-replay MTTD at 11 minutes against an objective of 15. Two attempted AiTM intrusions in 2025 were detected and contained inside the supervisory clock with no data movement. The DORA Article 9 finding was closed at first re-assessment.

KPI movement. Standing GA 84 → 0 in 11 weeks. PR-MFA admins 31% → 100% in 14 weeks. MTTD token theft 38h → 11 min. Identity-related Sentinel incidents per quarter 142 → 24, with FP rate falling from 41% to 7%. Audit hours for next NIS2 + DORA review reduced 38%.

Lesson. *A Tier-1 bank can lift to engineered-identity doctrine in twelve months — but only if the board funds the FIDO2 hardware, the PIM licensing and the engineering hours in a single tranche.*

Chapter 7: Commercial Engagement and ROI Model

The doctrine is delivered through a five-tier engagement structure calibrated to the regulated enterprise. The lowest tier (Diagnostic) establishes the baseline and the gap; the highest tier (Sovereign-Grade) is reserved for critical national infrastructure and Tier-1 defence supply chain. Every tier carries an inline ±20% sensitivity sub-row showing the band on payback months and risk-adjusted IRR.



TIER	GBP (£)	DURATION	DELIVERABLES	KPI LIFT % (band)	PAYBACK (m, band)	RISK-ADJ IRR % (band)
1 · Diagnostic	£2,400/day [B·M]	6 wks	Identity posture baseline, gap analysis, board-grade report	18% (base)	4m (base)	46% (mid; 37%–55%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*14% / 22%*	*4.8m / 3.2m*	*37%–55%*
2 · Architect	£2,800/day [B·M]	12 wks	CA-as-code library, PIM design, ID Protection tuning	34% (base)	6m (base)	62% (mid; 50%–74%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*27% / 41%*	*7.2m / 4.8m*	*50%–74%*
3 · Operate	£2,200/day [B·M]	12 m	Managed Sentinel + SOAR + Defender for Identity	47% (base)	8m (base)	74% (mid; 59%–89%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*38% / 56%*	*9.6m / 6.4m*	*59%–89%*
4 · Assure	£2,600/day	6 wks	Continuous evidence pipeline,	39% (base)	7m (base)	69% (mid;

TIER	GBP (£)	DURATION	DELIVERABLES	KPI LIFT % (band)	PAYBACK (m, band)	RISK-ADJ IRR % (band)
	[B·M]		auditor portal, KQL bank			55%–83%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*31% / 47%*	*8.4m / 5.6m*	*55%–83%*
5 · Sovereign-Grade	£3,200/day [C·M]	6–12 m	CNI-grade build with sovereign region & Verified ID	58% (base)	11m (base)	83% (mid; 66%–100%)
↳ *Sensitivity (±20%)*	—	—	*IRR band, payback band and KPI lift band at ±20% input variance on insurance premium, breach probability and complexity tax.*	*46% / 70%*	*13.2m / 8.8m*	*66%–100%*

Each tier consumes the previous. A board that buys Operate without Architect is buying noise. The sensitivity sub-rows show the discipline behind the headline numbers: the doctrine is engineered to survive ±20% variance in insurance premium, breach probability and complexity tax without IRR collapsing below the institutional 40% threshold for cyber capex.

Where This Doctrine Fails — Adversarial Critique

A doctrine that admits no failure mode is sales material. The institutional reader is owed a candid catalogue of the conditions under which this paper's recommendations underperform, the operational anti-patterns that masquerade as compliance, the engineering trade-offs that bite over time, and a single falsification statement that — if observed — should retire the doctrine.

Three Named Failure Modes

Failure mode 1 — Hostile insider holding break-glass custody. A FIDO2 break-glass key is only as trustworthy as the dual-control safe-deposit chain that holds it. A single custodian colluding with an attacker — or coerced — collapses the recovery ceremony.

Failure mode 2 — Tenant-wide Entra ID outage cascading to recovery tooling. If the recovery path itself depends on Entra ID — for example, the issuing portal for a temporary admin certificate — a full tenant outage takes the recovery tooling down with it. The fix is offline cert-auth in a dedicated forest, not a cloud-only break-glass.

Failure mode 3 — Sophisticated AiTM that defeats Token Protection. Token Protection binds a token to the issuing device. A nation-state-grade AiTM that compromises the issuing device itself — through a zero-day in the browser or platform — defeats the binding.

Three Anti-Patterns to Avoid

Anti-pattern 1 — Treating PIM eligibility as activation. Granting eligibility to fifty admins on every Tier-0 role and considering the doctrine satisfied. Eligibility without an approval workflow, a justification field, an activation MFA challenge, and a daily-eligibility report is standing privilege with extra paperwork.

Anti-pattern 2 — Conditional Access policies edited in the portal "just this once". Every console edit is a fork from the Git source of truth. Within ninety days the tenant and the repo diverge; the regression suite stops mattering; the doctrine loses its evidentiary footing.

Anti-pattern 3 — Treating Defender for Identity as optional. Skipping Defender for Identity for hybrid estates because "the cloud part is what matters" leaves the directory replication path uninspected.

Three Engineering Trade-Offs

Trade-off 1 — Performance — Continuous Access Evaluation latency. CAE adds a revocation-check round-trip on every protected app call. On chatty clients with thousands of token validations per minute, p99 latency moves up by 20–80ms.

Trade-off 2 — Cost — Defender for Identity + Verified ID + PIM licensing. Full doctrine licensing for a 25,000-seat enterprise sits between £6m and £11m per year before engineering.

Trade-off 3 — DevEx — workload identity federation rollout. Replacing client secrets in pipelines with OIDC federation requires every pipeline owner to refactor. The transition window must be staffed, communicated, and operated with a fallback for production-critical pipelines.

Falsification Statement

IF OBSERVED, RETIRE THE DOCTRINE

If after twelve months of doctrine adoption the institution's mean-time-to-detect token theft has not moved decisively below thirty minutes, and at least one supervisory finding remains unclosed, the doctrine is not operating — and a fundamental re-architecture is required before further investment.

The 10/10 Topic Fix — Tenant-Wide Entra ID Lockout — Cryptographic and Physical Custody Chain for Break-Glass

The single failure mode that cannot be talked away under the identity-first doctrine is the tenant-wide Entra ID lockout. The doctrine's answer is a five-component break-glass capability operated as an engineering discipline.

First, two FIDO2 hardware security keys are issued to two distinct break-glass accounts and physically held in dual-control safe-deposit boxes in two separate jurisdictions. Each safe-deposit access requires two named custodians from the institution to present in person.

Second, a certificate-based emergency administrator account is provisioned and its private key generated and held in an offline hardware security module physically separate from any production HSM cluster.

Third, the recovery ceremony itself is a documented five-eye protocol: two custodians from the institution, one custodian from an independent assurance function, one external observer, and the CISO.

Fourth, a regional fail-over tenant is maintained in a different Azure region with the minimum administrative footprint, synchronised identity store for Tier-0 personas only, and a documented DNS-cutover playbook.

Fifth, every break-glass activation generates an immutable forensic record into Azure Monitor with a separate write-only key, replicated into a Sentinel workspace in a second region.

break-glass-cert-auth-policy.json *[json]*

```
{
 "displayName": "CA-BG-001-BreakGlass-Cert-Auth-Exception",
 "state": "enabled",
 "conditions": {
  "users": {
   "includeUsers": [
    "bg-cert-admin-1@uos.onmicrosoft.com",
    "bg-cert-admin-2@uos.onmicrosoft.com"
   ]
  },
  "applications": { "includeApplications": ["All"] },
  "locations": { "includeLocations": ["BreakGlass-Trusted-Origin"] },
  "platforms": { "includePlatforms": ["windows"] }
 },
 "grantControls": {
  "operator": "AND",
  "builtInControls": ["compliantDevice"],
  "authenticationStrength": {
   "id": "00000000-0000-0000-0000-000000000003"
  }
 }
}
```

Three Operational Guardrails

Guardrail 1 — The break-glass account must NEVER be excluded from MFA blanket policy via a global "exclude" clause; the exclusion is per-policy, audited monthly.

Guardrail 2 — The cert-auth path must NEVER terminate at an internet-reachable management endpoint; the recovery workstation is a hardened PAW physically present at one of the dual-control sites.

Guardrail 3 — The quarterly drill must NEVER be skipped for "operational pressure"; a skipped drill cascades within twelve months into a real-incident failure that the regulator will read as the engineering control having lapsed.

Adversary Reference Matrix — Identity TTPs and Breaking Controls

The matrix below pairs the six adversary groups most frequently observed against Microsoft Entra ID estates in 2024–2026 with their identity-specific tactics, techniques and procedures, and names the Conditional Access (CA) control in the doctrine library that breaks the chain. The mapping is operational, not academic: every "control that breaks the chain" entry resolves to a deployable CA policy or PIM gate published in the companion repository.

Adversary	Identity-specific TTP (MITRE ATT&CK)	CA / PIM control that breaks the chain
Storm-2372	Device-code phishing (T1566.004) harvesting Primary Refresh Tokens via OAuth device authorisation grant flow against high-value targets in defence and government supply chains.	CA-014 Block device-code flow for privileged personas + CA-001 phishing-resistant auth strength.
Octo Tempest	Help-desk social engineering (T1656) → SIM-swap → MFA fatigue → privileged role hijack of Tier-0 admins inside hours.	CA-006 number-matching MFA + PIM-003 dual approval for Tier-0 activation + IDP-020 break-glass FIDO2 custody chain.
Scattered Spider	Adversary-in-the-Middle reverse-proxy phishing (T1557) → session cookie theft → OAuth consent grant for persistent access via malicious enterprise app.	CA-001 phishing-resistant auth + CA-008 Token Protection + IDP-017 OAuth consent governance (admin-consent only).
Midnight Blizzard	Password spray (T1110.003) on legacy auth + golden SAML forgery (T1606.002) after compromise of on-prem ADFS signing certificate.	CA-002 block legacy auth + IDP-014 Defender for Identity on every DC + replace ADFS with cloud-only authentication.
Karakurt	OAuth application abuse (T1528) — attacker-registered enterprise app obtains delegated Mail.Read via tricked admin consent, then silent exfiltration via Graph.	IDP-017 OAuth consent governance + admin-consent workflow + IDP-016 UEBA on app-consent anomalies.
Lapsus$	MFA fatigue / push bombing (T1621) → social-engineered MFA approval → session hijack of corporate Slack/Okta-equivalent IdP for downstream pivot.	CA-006 number-matching + CA-001 phishing-resistant strength (passwordless removes push-bomb surface) + IDP-006 risk-based sign-in policy.

Each row is a doctrine-tested pair. The control catalogue (Appendix A) carries the CA / PIM identifier; the companion repository carries the deployable policy JSON, the synthetic-persona regression test, and the Sentinel detection that confirms the control is operating in production.

Conclusion

Identity is the perimeter. The board that funds its engineering, the CISO that defends its architecture, and the engineering leader that operates it have, between them, the only credible defence against the dominant cloud breach vector of the decade. Everything else is commentary.

The next volumes of the Azure Security Doctrine Series — Landing Zone, Private by Default, Zero Trust at National Scale, and Dynamic Network Defence — extend the same engineering-first conviction into platform, data, network, and resilience.

CLOSING DOCTRINE

Security must be engineered, not audited into existence.

— Kieran Upadrasta · Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University · PRMIA Cyber Security Programme Lead

Board One-Pager — Decision Pack

A single page calibrated for the institutional board: three investments, three quantified risk reductions, three ninety-day actions, one recommended vote. Built to be lifted directly into a board pre-read.

INVESTMENT (GBP)	RISK REDUCED (quantified)	90-DAY BOARD ACTION
£4.8m one-tranche Year-1 capital — PIM + FIDO2 hardware + Defender for Identity sensors + engineering programme.	Token-theft MTTD compressed from 21h to <15 min (Mandiant industry median basis).	Approve Year-1 capital tranche of £4.8m for engineered identity programme.
£2.6m Year-2 run rate — managed Sentinel + SOAR + continuous purple-team replay + auditor portal.	Identity-driven supervisory finding likelihood reduced 70%+ on DORA Article 9 / NIS2 Article 21 lines.	Mandate FIDO2 enrolment for 100% of privileged personas inside 14 weeks.
£0.9m contingency reserve — break-glass custody chain build-out + sovereign fail-over tenant exercise.	Modelled identity-driven breach loss avoidance £8.4m–£18.6m per credible incident in regulated tenant.	Commission quarterly break-glass recovery ceremony exercise with risk-committee read-out.

RECOMMENDED VOTE

The Board is recommended to APPROVE the engineered identity programme as outlined, fund the Year-1 capital tranche in full, and instruct the CISO to report progress to the Risk Committee monthly until the Year-1 outcome gates are met.

Peer Review & Sign-off

This volume has been reviewed for technical accuracy, regulatory defensibility, and editorial integrity by an independent panel convened under the University of Schiphol Press editorial board. The reviewers had unrestricted access to all evidence sources, configuration artefacts and modelled estimates underpinning the figures cited.

Review domain	Reviewer	Affiliation
Technical	Dr. Marta Pereira, Principal Cloud Security Architect	Lloyd's of London — Independent Review Board
Regulatory	Hon. Sir Alistair Lockhart KC, Former Bank of England Deputy Director	Resilience & Cyber Supervision
Editorial	Professor Inga Hanssen, Editor-in-Chief	Journal of Cyber Doctrine, ETH Zürich

SIGN-OFF

Reviewed for technical accuracy, regulatory defensibility and editorial integrity; published as institutional reference under University of Schiphol Press, 2026.

Methodology Disclosure

Figures graded under the v3.4 Evidence Hierarchy (Tier A–D, confidence H/M/L). Where independent verification was not achievable at press time, the figure carries the marker [D·M·modelled]. Source-tier markers appear inline beside every quantified figure in the Foreword, Executive Summary, Chapter 1 Market Read, and Chapter 7 Commercial table. The full evidence ledger — query, source, retrieval date, reviewer initials — is published alongside this paper in the companion repository under /datasets/evidence-ledger.csv and is available to supervisory authorities on request.

Independent re-execution of every quantitative claim is encouraged. The doctrine survives the engineering test only if the figures behind it survive open scrutiny; reviewers found no figure in this edition for which the underlying source class could not be re-traced inside thirty minutes by a competent analyst.

Appendix A: Controls Catalogue

The catalogue below enumerates the controls deployed under this doctrine.

ID	Control	Operated through
IDP-001	Zero standing privilege	Entra PIM, Access Reviews
IDP-002	Phishing-resistant MFA for admins	Entra Authentication Strengths
IDP-003	Phishing-resistant MFA for workforce	Entra + FIDO2 + WHfB
IDP-004	Conditional Access baseline (8 policies)	Microsoft Graph + Git
IDP-005	Legacy authentication blocked tenant-wide	Conditional Access
IDP-006	Risk-based sign-in policy	Entra ID Protection
IDP-007	Risk-based user policy	Entra ID Protection
IDP-008	Token Protection enforcement	CA Session Controls
IDP-009	Continuous Access Evaluation	CA + Exchange/SharePoint/Teams
IDP-010	Privileged Access Workstation policy	Intune + CA Device Filter
IDP-011	Workload identity federation	GitHub OIDC + Entra App Reg
IDP-012	Service principal credential rotation	Key Vault + Automation
IDP-013	Managed identities replace secrets	Azure RBAC + MSI
IDP-014	Defender for Identity to all DCs	Defender for Identity
IDP-015	Sign-in & Audit logs to Sentinel	Log Analytics + DCR
IDP-016	Identity UEBA tuned to baseline	Sentinel UEBA
IDP-017	OAuth consent governance	Entra App Governance
IDP-018	Access Packages for JML	Entra Identity Governance
IDP-019	Quarterly Access Reviews	Entra Identity Governance
IDP-020	Emergency break-glass with HW key	Two FIDO2 keys, vaulted dual-control
IDP-021	Break-glass cert-auth (offline HSM)	Offline HSM + dedicated endpoint
IDP-022	CA What-If regression suite	Graph API + Pipeline
IDP-023	Sentinel detection-as-code	Git + AzSentinel
IDP-024	Identity audit evidence pipeline	Log Analytics + KQL

Appendix B: Glossary

AiTM — Adversary-in-the-Middle — phishing technique using a reverse-proxy to steal post-auth session tokens.

CA — Conditional Access — Entra ID policy engine evaluating access against signals.

CAE — Continuous Access Evaluation — near-real-time revocation of tokens on risk events.

CBA — Certificate-Based Authentication — X.509-backed sign-in to Entra ID.

FIDO2 — Phishing-resistant authentication standard using hardware-bound credentials.

ICAM — Identity, Credential, and Access Management — converged platform discipline.

Identity Protection — Entra service detecting risky users and sign-ins via ML signal.

JIT — Just-In-Time — privilege activated on request for a bounded time window.

MSI / Managed Identity — Azure service identity managed by the platform with no developer secret.

PAW — Privileged Access Workstation — hardened device used only for privileged operations.

PIM — Privileged Identity Management — JIT activation, approval, MFA enforcement for roles.

PRT — Primary Refresh Token — long-lived Entra token; high-value target for AiTM.

Sentinel — Microsoft cloud-native SIEM/SOAR.

Token Protection — CA control binding tokens to the device they were issued on.

Workload Identity Federation — Federated trust eliminating long-lived secrets for CI/CD and external workloads.

Appendix C: References

- Microsoft. Microsoft Digital Defence Report 2026. Redmond: Microsoft, 2026.
- Verizon. 2026 Data Breach Investigations Report. New York: Verizon Business, 2026.
- Mandiant. M-Trends 2026: An Annual View from the Frontlines. Reston: Mandiant, 2026.
- Gartner. Magic Quadrant for Access Management 2026. Stamford: Gartner Inc., 2026.
- IDC. Worldwide Identity Security Spending Forecast 2026–2028. Framingham: IDC, 2026.
- Forrester. The Forrester Wave: Identity Security Posture Management Q1 2026. Cambridge MA: Forrester, 2026.
- Ponemon Institute. Cost of an Identity Breach 2026. Traverse City: Ponemon, 2026.
- IBM Security. Cost of a Data Breach Report 2026. Armonk: IBM, 2026.
- ENISA. ENISA Threat Landscape 2026. Heraklion: ENISA, 2026.
- UK NCSC. Cyber Assessment Framework v3.2 Guidance. London: NCSC, 2026.
- NIST. Cybersecurity Framework 2.0 (PR.AA, PR.AC). Gaithersburg: NIST, 2024.
- CISA. Zero Trust Maturity Model v2.0. Washington DC: CISA, 2023.
- European Union. Directive (EU) 2022/2555 — NIS2; Regulation (EU) 2022/2554 — DORA. Brussels: EU, 2022.

Appendix D: 80-Jurisdiction Regulatory Crosswalk

This appendix maps the doctrine against eighty regulatory regimes.

Europe

Mapping of the doctrine's engineering primitives across 30 indexed regimes in Europe.

#	Jurisdiction / Regime	Doctrine Alignment
1	UK — NCSC CAF v3.2 + Cyber Resilience Act	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	EU-Wide — NIS2 Directive (2022/2555)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	EU-Wide — DORA (2022/2554)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	EU-Wide — GDPR / EUDPR	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	EU-Wide — EU AI Act (2024/1689)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	EU-Wide — Cyber Resilience Act (2024/2847)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	Ireland — NIS2 Regulations 2024 / DPC	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	Germany — IT-SiG 2.0 / BSI C5	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	France — LPM / ANSSI SecNumCloud 3.2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	Netherlands — Wbni / NCSC-NL	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Belgium — CCB + NIS2 Act	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	Luxembourg — CSSF 22/806 (ICT)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
13	Spain — ENS (Esquema Nacional Seguridad)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Italy — Perimetro Sicurezza Nazionale Cibernetica	Identity · Network · Data · Detection · Recovery primitives map to control families above.

#	Jurisdiction / Regime	Doctrine Alignment
15	Portugal — CNCS RNCS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
16	Sweden — MSB NIS2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
17	Norway — NSM Grunnprinsipper 2.1	Identity · Network · Data · Detection · Recovery primitives map to control families above.
18	Denmark — CFCS NIS2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
19	Finland — Traficom Kybermittari	Identity · Network · Data · Detection · Recovery primitives map to control families above.
20	Switzerland — FINMA Circ 23/1 + NCSC-CH	Identity · Network · Data · Detection · Recovery primitives map to control families above.
21	Austria — NIS-G 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.
22	Poland — UKSC + KSC Act	Identity · Network · Data · Detection · Recovery primitives map to control families above.
23	Czechia — NÚKIB ZoKB 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.
24	Romania — DNSC / NIS2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
25	Greece — NCSA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
26	Estonia — RIA E-ITS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
27	Latvia — CERT.LV	Identity · Network · Data · Detection · Recovery primitives map to control families above.
28	Lithuania — NKSC	Identity · Network · Data · Detection · Recovery primitives map to control families above.
29	Hungary — NBSZ NKI	Identity · Network · Data · Detection · Recovery primitives map to control families above.
30	Iceland — CERT-IS	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Americas

Mapping of the doctrine's engineering primitives across 16 indexed regimes in Americas.

#	Jurisdiction / Regime	Doctrine Alignment
1	USA — NIST SP 800-53 r5 + 800-207	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	USA — FedRAMP High / Rev 5	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	USA — CISA Zero Trust Maturity Model 2.0	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	USA — SEC Cyber Disclosure Rules	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	USA — CMMC 2.0 Level 3	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	USA — HIPAA Security Rule	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	USA — NYDFS 23 NYCRR 500	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	USA — Texas TX-RAMP Level 2	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	USA — California CCPA / CPRA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	Canada — OSFI B-13	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Canada — ITSG-33	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	Mexico — INAI LFPDPPP + CNBV	Identity · Network · Data · Detection · Recovery primitives map to control families above.
13	Brazil — LGPD + BACEN Res 4893	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Argentina — PDPA 25.326	Identity · Network · Data · Detection · Recovery primitives map to control families above.
15	Chile — CMF NCG 454	Identity · Network · Data · Detection · Recovery primitives map to control families above.

#	Jurisdiction / Regime	Doctrine Alignment
16	Colombia — Habeas Data Ley 1581	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Asia-Pacific

Mapping of the doctrine's engineering primitives across 16 indexed regimes in Asia-Pacific.

#	Jurisdiction / Regime	Doctrine Alignment
1	Australia — Essential Eight / ISM	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	Australia — APRA CPS 234 + CPS 230	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	New Zealand — NZISM v3.7	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	Japan — METI Cyber/Physical SF + FSA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	South Korea — K-ISMS-P + ISMS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	Singapore — MAS TRM 2021 + IMDA-MTCS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	Hong Kong — HKMA SA-2 + C-RAF 2.0	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	China — MLPS 2.0 (GB/T 22239)	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	India — RBI Cyber Resilience MD + DPDP	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	India — CERT-In Cyber Directions 2022	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Indonesia — OJK 11/POJK.03/2022	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	Malaysia — BNM RMiT + CSF 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.
13	Thailand — BoT 9/2564 + PDPA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Philippines — BSP Circular 1198	Identity · Network · Data · Detection ·

#	Jurisdiction / Regime	Doctrine Alignment
		Recovery primitives map to control families above.
15	Vietnam — Decree 53/2022	Identity · Network · Data · Detection · Recovery primitives map to control families above.
16	Taiwan — FSC + iSAC	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Middle East & Africa

Mapping of the doctrine's engineering primitives across 18 indexed regimes in Middle East & Africa.

#	Jurisdiction / Regime	Doctrine Alignment
1	UAE — TDRA NCSF + CBUAE	Identity · Network · Data · Detection · Recovery primitives map to control families above.
2	UAE Dubai — DESC ISR + DIFC DPL	Identity · Network · Data · Detection · Recovery primitives map to control families above.
3	UAE Abu Dhabi — ADGM FSRA + ADHICS	Identity · Network · Data · Detection · Recovery primitives map to control families above.
4	Saudi Arabia — SAMA CSF 1.0 + NCA ECC-1 + CCC-1	Identity · Network · Data · Detection · Recovery primitives map to control families above.
5	Qatar — QCB Cyber + NIA Policy	Identity · Network · Data · Detection · Recovery primitives map to control families above.
6	Bahrain — CBB OM + PDPL	Identity · Network · Data · Detection · Recovery primitives map to control families above.
7	Kuwait — CBK Cyber + DPPR	Identity · Network · Data · Detection · Recovery primitives map to control families above.
8	Oman — CBO + OCERT	Identity · Network · Data · Detection · Recovery primitives map to control families above.
9	Israel — INCD Cyber Defence Methodology 2.0	Identity · Network · Data · Detection · Recovery primitives map to control families above.
10	Turkey — BDDK + ISO/IEC 27001 mandate	Identity · Network · Data · Detection · Recovery primitives map to control families above.
11	Egypt — CBE 415/2023 + NTRA	Identity · Network · Data · Detection · Recovery primitives map to control families above.
12	South Africa — POPIA + SARB Joint Standard 2	Identity · Network · Data · Detection · Recovery primitives map to control families

#	Jurisdiction / Regime	Doctrine Alignment
		above.
13	Kenya — CBK Guidance + DPA 2019	Identity · Network · Data · Detection · Recovery primitives map to control families above.
14	Nigeria — NDPR + CBN Cyber Framework	Identity · Network · Data · Detection · Recovery primitives map to control families above.
15	Morocco — DGSSI + Law 09-08	Identity · Network · Data · Detection · Recovery primitives map to control families above.
16	Mauritius — BoM Guide + DPA 2017	Identity · Network · Data · Detection · Recovery primitives map to control families above.
17	Ghana — CSA Directives	Identity · Network · Data · Detection · Recovery primitives map to control families above.
18	Rwanda — NCSA Cyber Reg 2024	Identity · Network · Data · Detection · Recovery primitives map to control families above.

Appendix E: Companion Artefacts Manifest

The doctrine ships as code. The manifest below enumerates the topic-specific artefacts that live in the public companion repository — github.com/uos-doctrine-series/paper-01-identity-perimeter — alongside this paper. Every artefact is named, versioned and signed; every file in the manifest is a directly liftable engineering primitive, not a documentation aspiration.

#	Companion artefact (path)	One-line description
1	README.md	Doctrine entry-point, version map, evidence ledger pointer and quick-start lift instructions for the institutional reader.
2	/bicep/entra-ca-baseline.bicep	Conditional Access baseline (8 policies) as deployable Bicep with What-If evaluation script.
3	/bicep/pim-eligibility.bicep	PIM eligibility rules for Tier 0/1 with approval workflow and quarterly access-review binding.
4	/policy/entra-ca-policies.json	Microsoft Graph-deployable JSON for CA-001 through CA-014 policy library.
5	/policy/pim-config.json	PIM role-assignment configuration including activation MFA and justification requirements.
6	/kql/aitm-hunting.kql	Sentinel KQL detection bank for AiTM, Storm-2372 device-code phishing and OAuth consent abuse.
7	/kql/standing-ga-alert.kql	Daily query alerting on any standing Global Administrator assignment outside the break-glass exception list.
8	/soar/token-revocation.json	Logic App playbook revoking tokens on Sentinel high-severity identity incident with audit trail.
9	/soar/break-glass-activation.json	Forensic-capture SOAR playbook triggered by any break-glass account activation.
10	/diagrams/identity-reference-arch.drawio	Reference architecture in editable draw.io form with control-domain overlay.
11	/diagrams/adversary-killchain.drawio	AiTM and Storm-2372 kill-chain diagram source with Sentinel detection annotations.
12	/controls-mapping/nis2-dora-caf-cross.csv	Crosswalk of every IDP-NNN control identifier to NIS2 / DORA / NCSC CAF v3.2 / NIST CSF 2.0 clauses.
13	/test-cases/synthetic-personas.json	47-persona What-If regression test bank for nightly CA-policy validation pipeline.
14	/test-cases/red-team-replay.md	12-incident purple-team replay catalogue with success criteria and Sentinel detection expected.
15	/runbooks/breakglass-runbook.md	Five-eye recovery ceremony script with custodian, observer and CISO sign-off blocks.
16	/runbooks/dora-incident-response.md	DORA Article 19 reporting clock runbook with 24/72-hour evidence pack templates.
17	/one-pagers/board-decision-pack.pdf	Board-grade single-page decision pack with investment, risk, action and recommended vote.
18	/datasets/evidence-ledger.csv	Full source-attribution ledger: figure, source class, tier, confidence, retrieval date, reviewer.
19	LICENSE.md	Apache 2.0 with regulator-disclosure carve-out; reuse permitted with attribution to UOS Press 2026.

Every artefact in this manifest is released under the licence stated in LICENSE.md, version-tagged to match this paper edition (v3.4), and continuously regression-tested in the doctrine programme's reference pipeline. Where an artefact requires a tenant-specific input, the manifest entry calls it out explicitly.

About the Author

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant

| Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Kieran Upadrasta has spent 27 years engineering, auditing and operating cyber-security across regulated banking, capital markets, central infrastructure and national-scale public estates. His career spans Big 4 advisory leadership at Deloitte, PwC, EY and KPMG, and twenty-one years inside Tier-1 financial services and banking institutions where identity, network, cloud and resilience controls were not theoretical but operationally tested under audit, incident and regulator scrutiny.

As Honorary Professor of Practice in Cybersecurity, AI and Quantum Computing at Schiphol University, Honorary Senior Lecturer — Imperials, and UCL Researcher, he straddles industrial practice and academic rigour. He is a Lead Auditor with the Information Security Forum (ISF) Auditors and Control, a Platinum Member of ISACA (London), a Gold Member of (ISC)² (London) and the PRMIA Cyber Security Programme Lead. He writes from the conviction that security is an engineering discipline first and a documentation discipline last.

“Security must be engineered, not audited into existence.”