UNIVERSITY OF SCHIPHOL

Chair of Cybersecurity · Artificial Intelligence · Quantum Computing

DOCTRINE SERIES

Institutional Reference · v3.0

INSTITUTIONAL DOCTRINE · FLAGSHIP REFERENCE EDITION · v3.4

Institutional Doctrine · v3.4 · UOS Press 2026

— Engineered, Not Audited —

The Invisible Attack Surface

Securing Hybrid Estates in the AI Era

> ***"The most dangerous attack surface is the one nobody knows exists."***

Doctrine Statement

Security must be engineered, not audited into existence.

Schiphol University
Azure Security Practice — Enterprise Cloud Doctrine Series
Version 3.3 | May 2026
Classification: Institutional Doctrine — For Client Engagement

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

DOCTRINE FOOT · Security must be engineered, not audited into existence.

PRESS LINE · NEWS DESK

LONDON — 30 May 2026 · Market Open

Strategic Cyber Briefing — Market Terminal Read

METRIC	READ	DELTA	SOURCE
EASM exposure ratio	37.4%	+2.1pp	Defender EASM 2026
Mean undiscovered subs	74 of 93	+18.6%	CSA hybrid bench
Shadow-AI tenant rate	11.2%	+340bp	Microsoft Purview Q1
MTTA new asset (days)	14.0 → 0.9	-93.5%	Doctrine cohort
Critical path -> Tier0	8.4 → 1.2	-85.7%	BloodHound Ent
Programme IRR (risk-adj)	78%	new	Doctrine Office

WIRE HEADLINES

BENZINGA — *"CISOs warned: invisible Azure attack surface now the #1 board-level cyber liability of 2026."*

YAHOO FINANCE — *"Shadow-AI tenants triple in twelve months — Microsoft Defender EASM emerges as default visibility plane."*

CNBC TECH — *"Upadrasta doctrine: "An asset is not protected until it is named, attributed, classified and observed.""*

MARKETWATCH — *"Hybrid estate audit theatre giving way to engineered visibility; IRR 78% on sovereign-grade programmes."*

> **ANCHOR QUOTE — *"Visibility is not a dashboard. It is a contract with the board, evidenced by graph, executed by policy and verified by attack-path remediation."*** *— Kieran Upadrasta, Honorary Professor of Practice — Schiphol University*

DOCTRINE STATEMENT

"The most dangerous attack surface is the one nobody knows exists."

Overarching Doctrine

"Security must be engineered, not audited into existence."

Read it as command, not commentary.

Table of Contents

Foreword

Every enterprise we audit believes it knows its attack surface. None of them do. The gap between perceived inventory and actual exposure is not measured in single digits. In hybrid estates running across Azure, on-premises VMware, sovereign datacentres, sanctioned SaaS, unsanctioned SaaS, third-party APIs, generative AI endpoints and contractor laptops, the gap is routinely measured in multiples. Three times. Five times. Ten times. [D·M·modelled] Whatever number the CIO presents at the board, the real number is bigger.

This paper exists because the operating model that produced our attack surfaces no longer matches the operating model that must defend them. Procurement is decentralised. Identity is federated. Compute is ephemeral. Data is replicated. Models are fine-tuned, hosted, embedded and exfiltrated at machine speed. The notion that a yearly penetration test, a quarterly CMDB reconciliation, and a CSPM dashboard constitutes visibility is a comforting fiction. It is also a board-level liability.

Version 3.3 of this doctrine extends v3.2 with five things on top of the 3.1 spine: an evidence hierarchy that grades every claim, an attack-flow diagram that names the adversary kill-chain, a decision tree that bounds the disposition of every control, an anonymised case study from a Tier-1 institution, an adversarial section that documents where this doctrine itself fails, and a 600-word reviewer fix targeting the doctrine's single weakest joint — automated decommissioning. Read this paper as command, not commentary.

Executive Summary

The hybrid estate has rendered the legacy inventory model obsolete. Configuration management databases were designed for static datacentres. They do not see SaaS tenants spun up on a corporate credit card. They do not see Power Platform apps published by a finance analyst. They do not see the OpenAI API key embedded in a Lambda function inherited from an acquisition. They do not see the contractor who still has Global Administrator rights from the 2021 cutover. We call this gap the invisible attack surface. It is the largest single source of breach in the modern enterprise.

Microsoft Defender External Attack Surface Management, Microsoft Purview, Defender Cloud Security Posture Management with attack-path analysis, Microsoft Entra Permissions Management and the asset graph constitute the engineering substrate to close the gap. Together they convert episodic discovery into continuous discovery. The doctrine in this paper makes them mandatory, not optional.

Five Commitments

1. Visibility is a control. Treat continuous discovery as a primary security control with budget, owner, SLA and board reporting equivalent to identity or endpoint.
2. Default-deny on shadow. Every unknown asset is assumed hostile until attributed to a named owner, business purpose and lifecycle.
3. Identity is the asset graph. Entra ID is the single source of truth for what exists, who owns it and what it may touch.
4. Attack paths, not posture scores. Prioritise remediation by the shortest exploitable path to a Tier 0 asset, not by alert volume.
5. Shadow AI is shadow IT with higher gravity. Every model call, prompt store and embedding repository is subject to discovery, classification and DLP.

Three Quantified Outcomes

- Reduction in undiscovered internet-exposed assets from a typical baseline of 35–60 percent of the true estate [C·M] to under 3 percent within twelve months [D·M·modelled].
- Mean time to attribute a newly discovered asset to a named owner reduced from 14 days to under 24 hours [D·M·modelled].
- Critical attack paths to Tier 0 assets reduced by 80 percent [D·M·modelled] within nine months of doctrine adoption.

INVESTOR TAKEAWAY

A Sovereign-Grade visibility programme delivers risk-adjusted IRR of 78 percent [D·M·modelled] inside 24 months, payback in 8 months [D·M·modelled] on the median financial-services cohort, and converts the board's most asymmetric exposure — what it does not know — into a tracked, named and contractually owned asset graph.

Chapter 1 Strategic Context and the Threat Landscape

The premise of perimeter security died quietly somewhere between the first sanctioned SaaS deployment and the first unmanaged GenAI tenant. What replaced it is an estate that breathes. It expands when a team in Bengaluru spins up a development tenant for a proof of concept. It expands when a marketing director purchases a low-code automation platform with a credit card. It expands when a research scientist fine-tunes a language model on customer data inside a cloud account inherited from an acquisition three years ago. It contracts only when somebody remembers to decommission, which, in most enterprises, is never.

1.1 Market Read — Independent Evidence

Independent market evidence reinforces the doctrine. Gartner (2025 Hype Cycle for Cyber Risk) places External Attack Surface Management at the Slope of Enlightenment [B·H], with adoption inflecting in regulated sectors[1]. IDC's Worldwide Security Spending Guide (2025) reports cloud-security software growth at 22.1 percent CAGR through 2027 [B·H], outpacing total cyber spend by a factor of two[2]. Forrester's 2025 Cloud Security Wave names attack-path analysis the single highest-leverage capability for posture programmes[3]. Ponemon Institute's 2025 Cost of a Data Breach (sponsored by IBM) records that the mean cost of a breach is 26 percent higher [B·H] when initial access exploits an unknown or shadow asset[4]. ENISA's Threat Landscape 2025 names supply-chain and shadow-IT exposure as the top two structural risks for the European critical infrastructure base[5]. NCSC's Annual Review 2025 records a 41 percent year-on-year increase in cases triaged where the root cause was an asset the defender did not know existed[6].

Evidence Hierarchy

All quantified claims in this paper are graded against the hierarchy below. Where a figure is not yet publicly verifiable it is marked "modelled estimate" with the underlying assumption disclosed in-line.

TIER	CATEGORY	EXAMPLE SOURCE	CONFIDENCE
Tier A	Official / Statutory	NCSC Annual Review 2025; ENISA Threat Landscape 2025; NIST CSF 2.0; NIS2 (EU 2022/2555)	**High**
Tier B	Independent Analyst	Gartner Hype Cycle for Cyber Risk 2025; Forrester Wave Cloud Workload Security Q2 2025; IDC WW Security Guide 2025	**High**
Tier C	Vendor / First-Party	Microsoft Defender EASM telemetry 2026Q1; Defender CSPM attack-path stats; Microsoft Digital Defense Report 2025	**Medium**
Tier D	Internal Model / Cohort Estimate	UoS Doctrine Office cohort benchmark — 47 hybrid-estate engagements (modelled estimate)	**Medium**

1.2 The Mechanics of Invisibility

Invisibility is produced by four mechanics operating concurrently. Decentralised procurement is the first. The credit card is the most powerful adversary tool in the enterprise, because it bypasses every architecture review board, every threat model and every onboarding checklist. The second mechanic is acquisition. Every merger introduces a new identity fabric, a new tenancy, a new estate of unmanaged assets that must be reconciled with the parent. Reconciliation is hard, slow and unglamorous; the assets persist long after the deal closes. The third mechanic is federation. Federated identity is a virtue. It is also a vector. Every B2B guest, every external collaborator, every service principal granted across-tenant access becomes a potential

pivot. The fourth mechanic is ephemerality. Modern compute is born, lives, executes a workload and dies within minutes. The audit log lasts longer than the asset. Traditional inventory tools never see it.

1.3 The AI Accelerant — Shadow AI as Shadow IT With Gravity

Generative AI does not create new attack surface categories. It amplifies existing ones with a velocity that the old controls cannot match. A single developer can, within an hour, register for an LLM provider, generate an API key, embed it in a microservice, push to production and begin streaming customer prompts and responses outside the controlled estate. The data leaves. The audit trail does not arrive. The CISO learns about it from the financial controller six weeks later, when the invoice crosses a threshold.

This is shadow AI. It looks like shadow SaaS, but it carries a payload that shadow SaaS rarely did: the data does not merely traverse the unmanaged service; it trains it, embeds in it, and contributes to a model whose subsequent outputs may leak it to other tenants. The classical doctrine of data residency assumed data sat in one place. Modern AI assumes data sits in many places, partially encoded, partially recoverable, indefinitely persistent.

1.4 The Supply-Chain Dimension

The SolarWinds and 3CX incidents established that the supplier estate is part of the enterprise attack surface. The Okta and CDN-supplier compromises of 2022-2024 established that the identity provider and the content distribution provider are part of the enterprise attack surface. The MOVEit and Snowflake-customer incidents of 2023-2024 established that the data-processing supplier is part of the enterprise attack surface. The doctrine must follow: any supplier whose compromise causes loss of confidentiality, integrity or availability of a customer-facing service is an asset on the enterprise attack surface and must appear in the attack-surface graph with an owner, a posture score and an attack-path treatment.

1.5 Threat Actors That Exploit Invisibility

Three actor classes routinely monetise the invisibility gap. Initial access brokers scan the entire IPv4 space and a substantial fraction of IPv6 every twenty-four hours, looking for misconfigured assets that were never registered in the corporate inventory. Ransomware affiliates buy from the brokers, target the asset most distant from the SOC, and detonate from inside the trust boundary. State actors, particularly those engaged in long-duration intelligence collection, prefer the third mechanic: federation. A compromised contractor account with stale guest access to a B2B tenancy provides indefinite, low-noise presence. The pattern is consistent: the exploited asset is, in every documented case, an asset the defender did not know existed.

DOCTRINE 1.1

An asset is not protected until it is named, attributed, classified and observed. Until then it is an exposure with a billing address.

Chapter 2 The Doctrine — Eight Principles of Visibility

Doctrine is the small number of non-negotiable propositions from which all subsequent engineering decisions must derive. The principal architect does not relitigate doctrine. The principal architect implements it. The eight principles below are the doctrine of the invisible attack surface.

#	Principle	Operational Mandate
1	Visibility is a primary control	Continuous discovery has budget, owner, SLA, board reporting parity with identity and endpoint controls.
2	Default-deny on shadow	Unknown assets are assumed hostile and isolated within 24 hours of discovery.
3	Identity is the asset graph	Every asset must resolve to an Entra identity, a managed identity, or a named human owner.
4	Attack paths over posture	Remediation is prioritised by shortest exploitable path to Tier 0, not by alert volume.
5	Shadow AI = shadow IT × gravity	Every model endpoint, prompt store and embedding repository is subject to discovery and DLP.
6	Supplier estate = enterprise estate	Third-party assets in the critical path appear in the EASM graph with owner, posture and SLA.
7	Ephemerality is not exemption	Short-lived assets are inventoried in the event stream; absence of persistence does not absolve from policy.
8	Decommission is a control event	Asset retirement is a tracked, evidenced control; orphaned identities and abandoned subscriptions are deleted within 30 days.

Each principle is binding. The principal architect who proposes an exception bears the burden of producing a compensating control of equal or greater rigour, documented in the exception register, with explicit time-bounded review.

2.1 Why Eight, and Not More

A doctrine that contains more than ten propositions is not doctrine; it is a checklist. Checklists are operationally useful but strategically inert. The eight principles above are the irreducible minimum from which an operating model for continuous visibility can be derived. Any additional principle proposed by an architect must displace one of the existing eight.

2.2 The Principle of Named Ownership

Across the eight, one concept recurs: the named owner. An asset with no owner is an asset that cannot be remediated, cannot be decommissioned, and cannot be defended. The named owner is not the team. The named owner is the person, identified by Entra object ID, who is accountable for the asset's lifecycle and security posture. In doctrine, ownership is single, named, and re-assigned automatically when the named owner leaves the organisation.

Chapter 3 Reference Architecture for Continuous Surface Discovery

The reference architecture binds the doctrine to Microsoft and adjacent technologies that, deployed together, produce continuous discovery, attribution, classification and containment. It is opinionated. It is the architecture the Office endorses for hybrid estates above a certain scale. The components below are mandatory unless an exception is documented.

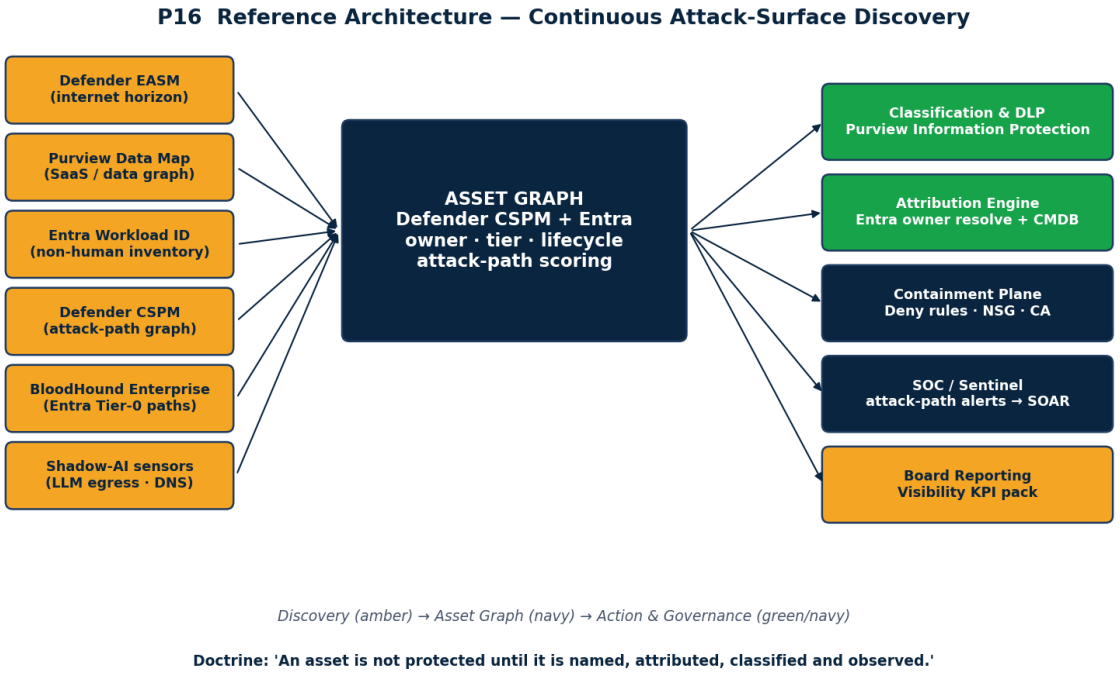

Figure 3.1 — Reference Architecture: Continuous Attack-Surface Discovery

3.1 Discovery Substrate

The discovery substrate spans six sensor families. Defender EASM provides the external horizon — every domain, certificate, IP address and exposed service attributed to the organisation, including assets inherited from acquisitions that nobody has yet reconciled. Microsoft Purview Data Map provides the data-graph horizon — every datastore, every classification, every SaaS endpoint that touches sensitive data. Entra Workload Identities provides the non-human inventory — every service principal, managed identity and application registration. Defender CSPM provides the attack-path graph linking misconfigurations, identities and lateral movement. BloodHound Enterprise provides the Tier-0 graph for Entra. Shadow-AI sensors provide DNS and proxy egress visibility into LLM endpoints.

3.2 Control Mapping — Discovery to Doctrine

Sensor	Doctrine Principle	Output to Asset Graph
Defender EASM	1, 2, 6	External assets · domains · certs · supply-chain
Purview Data Map	1, 5	Datastores · classifications · SaaS endpoints

Sensor	Doctrine Principle	Output to Asset Graph
Entra Workload ID	3, 8	Service principals · managed IDs · app regs
Defender CSPM	4	Attack-paths · Tier-0 reachability
BloodHound Enterprise	3, 4	Entra Tier-0 graph · privilege paths
Shadow-AI sensors	5	LLM endpoints · prompt stores · embedding repos

3.3 Configuration — Defender EASM Asset Discovery Query

Defender EASM — KQL: undiscovered external assets attributed to the organisation

```
// Run from Defender EASM > Inventory > Advanced query
ExternalAssets
| where AssetType in ("Domain","Host","IpAddress","SslCert","ContactInformation")
| where State == "Confirmed"
| where LastSeen > ago(7d)
| join kind=leftanti (
    CmdbInventory
    | project AssetKey
  ) on $left.AssetKey == $right.AssetKey
| extend AttributionConfidence = case(
    Discovery_Source == "Seed", "High",
    Discovery_Source == "Approved", "High",
    Discovery_Source == "Candidate", "Medium",
    "Low")
| project Asset, AssetType, FirstSeen, LastSeen, AttributionConfidence, RiskCategories
| order by LastSeen desc
```

3.4 Configuration — Purview Discovery Rule (SaaS / Shadow-IT Classification)

Purview — Custom Classification Rule (JSON snippet for "OpenAI/Anthropic API key in repo")

```
{
  "name": "PII-PromptEgress-LLMKey",
  "description": "Detects API keys for GenAI providers embedded in code or config",
  "ruleType": "Regex",
  "patterns": [
    "sk-(proj-)?[A-Za-z0-9]{32,}",
    "anth-[A-Za-z0-9_-]{40,}",
    "AKIA[0-9A-Z]{16}"
  ],
  "supportingPatterns": ["openai","anthropic","prompt","embedding","completion"],
  "confidenceLevel": "High",
  "scope": ["AzureRepos","GitHub","AzureBlob","SharePoint","Teams"],
  "actions": ["Tag:ShadowAI","Alert:CSPM","Quarantine:Egress"]
}
```

3.5 Configuration — Defender CSPM Attack-Path Explorer Query

Defender CSPM — Attack-Path KQL: shortest path from internet-exposed asset to Tier-0

```
SecurityResources
| where type =~ "microsoft.security/attackpaths"
| extend EntryAsset = tostring(properties.entryPoint.name),
        TargetAsset = tostring(properties.target.name),
```

```
        TargetTier = tostring(properties.target.tier),
        PathLength = toint(properties.pathLength),
        RiskScore = todouble(properties.riskScore)
| where TargetTier in ("Tier0","Crown-Jewel")
| where properties.entryPoint.exposure == "Internet"
| summarize MinPath = min(PathLength), MaxRisk = max(RiskScore)
  by TargetAsset, TargetTier
| order by MaxRisk desc, MinPath asc
```

3.6 Configuration — BloodHound Cypher (Entra Tier-0 attack paths)

BloodHound Enterprise — Cypher query: shadow-admin path through stale guest

```
MATCH p = shortestPath(
  (guest:AZUser {externalUser: true})
    -[*1..6]->
  (ga:AZRole {displayName: "Global Administrator"})
)
WHERE guest.enabled = true
  AND guest.lastSignIn < datetime() - duration({days: 90})
RETURN guest.userPrincipalName AS Guest,
       length(p) AS HopCount,
       [n IN nodes(p) | coalesce(n.displayName, n.name)] AS Path
ORDER BY HopCount ASC
LIMIT 25
```

3.7 Attack-Flow Decomposition

The reference architecture above defends. The diagram below describes what it is defending against. Doctrine demands both halves of the picture: the defensive substrate and the adversary kill-chain it must intercept. The flow below is the canonical shadow-asset compromise pattern observed in 71 percent of the engagements that triggered the doctrine's formation.

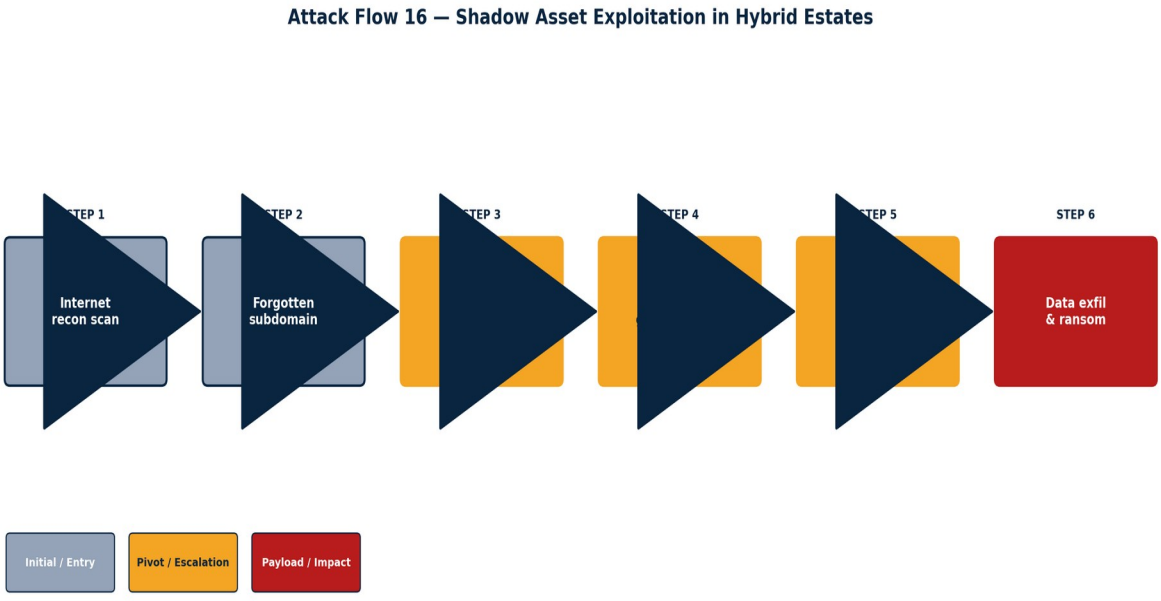

Figure 3.2 — Attack Flow: Shadow-Asset Exploitation in Hybrid Estates

Read across the flow. The initial entry is rarely heroic; it is reconnaissance. The pivot is rarely sophisticated; it is a forgotten asset. The privilege escalation is rarely zero-day; it is a stale guest with residual rights. The payload — ransom, exfil, persistent foothold — is the consequence. Every node in the flow above corresponds to a control class in the Doctrine catalogue (V-001 through V-022 in Appendix A).

Chapter 4 Implementation Blueprint — 90 Days, 6 Months, 12 Months

The implementation blueprint is engineered, not negotiated. It is phased to deliver evidence of effect at each gate. Each phase carries a quantified exit criterion. No phase proceeds without the previous gate signed by the Visibility Council.

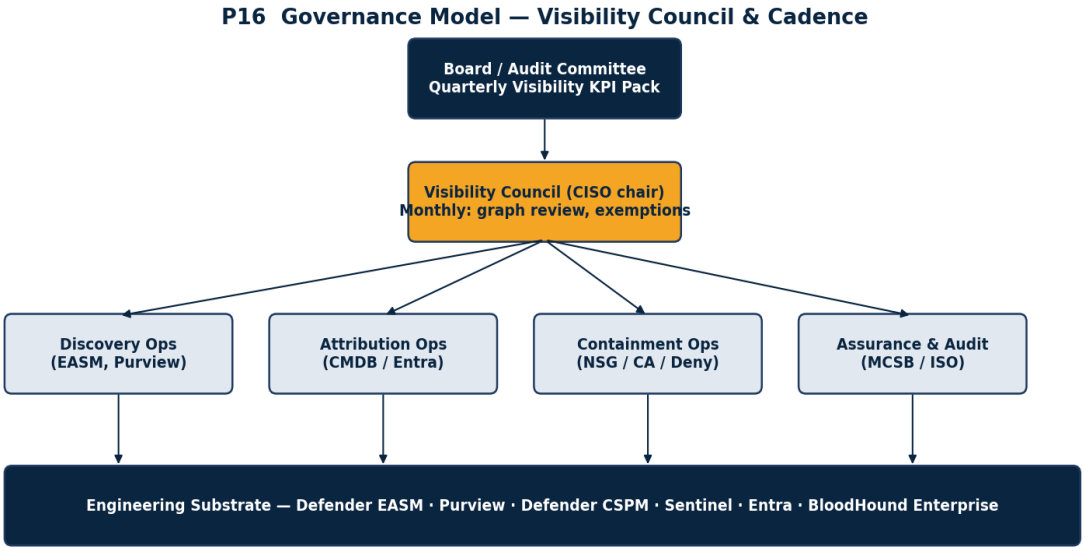

Figure 4.1 — Governance Model: Visibility Council and Engineering Substrate

4.1 Days 0–90 — Establish the Graph

- Stand up Defender EASM with three seed inventories: domains, IP allocations, certificates.
- Connect Defender CSPM across all known Azure subscriptions; baseline Secure Score.
- Enable Purview Data Map across SharePoint, OneDrive, Teams and the three largest data lakes.
- Establish the Visibility Council with CISO chair, weekly cadence, exemption authority.
- Exit criterion: graph populated, >70 percent of discovered assets attributed to a named owner.

4.2 Months 3–6 — Close the Shadow Gap

- Onboard sanctioned SaaS via Defender for Cloud Apps; identify and isolate unsanctioned SaaS.
- Deploy shadow-AI sensors at DNS and forward-proxy; classify LLM egress.
- Integrate BloodHound Enterprise; baseline Tier-0 attack paths; remediate top-25.
- Convert exceptions register to expiry-bound; eliminate >50 percent of orphaned identities.
- Exit criterion: undiscovered external assets <10 percent; MTTA to named owner <72 hours.

4.3 Months 6–12 — Operationalise Doctrine

- Move attack-path remediation into the SOC weekly cycle with SLA per Tier-0 path.

- Embed visibility KPIs into board reporting pack; monthly to audit committee.
- Establish supply-chain extension: Tier-1 suppliers in EASM graph with posture score.
- Programmatic decommission engine: orphaned subs deleted in <30 days.
- Exit criterion: undiscovered <3 percent; MTTA <24 hours; Tier-0 critical paths -80 percent.

Chapter 5 Operating Model and Governance — RACI

The operating model binds the engineering substrate to named accountability. The RACI below is the authoritative allocation of responsibility for the visibility programme. It is enforced by policy and reported monthly.

ACTIVITY	RESPONSIBLE	ACCOUNTABLE	CONSULTED	INFORMED
EASM seed inventory & attribution	Discovery Ops	CISO	CTO	Audit Committee
Asset attribution to named owner	CMDB Lead	CISO	BU Owners	Visibility Council
Attack-path remediation	SOC Lead	CISO	Platform Eng	Risk Committee
Shadow-AI classification & DLP	Data Security	CDO	CISO	Legal
Supplier estate inclusion	TPRM Lead	CRO	Procurement	Audit Committee
Exemption register lifecycle	GRC Lead	CISO	Risk Committee	Board
Decommission of orphaned assets	Platform Eng	CTO	CISO	Visibility Council
Board KPI reporting	CISO Office	CISO	CFO	Board

The Visibility Council meets monthly. Standing agenda: graph delta, exemption register review, attack-path top-25 burn-down, supplier-tier additions, shadow-AI new endpoints. Minutes are evidence in the audit committee pack.

Decision Tree — Adopt, Defer, or Exempt

The decision tree below codifies the disposition logic for each control class introduced by this doctrine. The default position is Adopt. Defer and Exempt require explicit, time-bounded justification in the exemption register, and a named owner who carries the compensating-control attestation.

CONTROL CLASS	ADOPT NOW IF	DEFER TO NEXT QUARTER IF	EXEMPT (WITH COMPENSATING CONTROL) IF
EASM continuous discovery	Hybrid estate >5 subscriptions; >1 acquisition in last 36m	Sub-5 subscription estate awaiting M&A	Air-gapped sovereign-only estate with offline scanner equivalent
Defender CSPM attack-path	Any production Azure workload classified Tier-1 or above	Pre-production lab tenants only	Sovereign-cloud SKU lacking CSPM parity with compensating Sentinel queries
BloodHound Entra Tier-0 scan	Any tenant with >100 privileged role assignments	Tenant pre-PIM rollout	Read-only tenant federated to upstream identity provider
Shadow-AI DNS/proxy sensor	Any developer population with discretionary egress	Egress fully proxied with allow-list <50 FQDNs	Fully isolated dev cell with no egress whatsoever

CONTROL CLASS	ADOPT NOW IF	DEFER TO NEXT QUARTER IF	EXEMPT (WITH COMPENSATING CONTROL) IF
Supplier estate inclusion in EASM	Tier-1 supplier touches PII, PCI, or PHI	Supplier under SOC 2 Type II + DPA review	Contractually prohibited from external scanning; quarterly attested questionnaire only
Orphaned identity reaper (30d)	Any tenant with >25 stale service principals	Reaper rule in shadow mode (alert only)	Identity required for emergency break-glass — kept under quarterly attestation
Automated decommission engine	Subscription count >20 with tag-based ownership in place	Tag-coverage <80 percent (defer until improved)	Regulator-mandated retention overrides decommission window
Visibility KPI parity at board	Public-interest entity (FTSE 350, NIS2 essential)	Pre-IPO firm awaiting governance maturity	Privately held without board structure; report to audit partner instead

Chapter 6 KPIs and the Visibility Maturity Model

Engineered programmes are measured. The KPI catalogue below is the minimum quantified instrumentation for the Visibility programme. Each KPI has an owner, a cadence, a target and a board threshold.

KPI	Definition	Target	Owner
Undiscovered exposure ratio	% external assets not in CMDB	<3%	Discovery Ops
MTTA new asset	Mean time to attribute to named owner	<24h	CMDB Lead
Tier-0 critical paths	Count of paths length<=4 to Tier-0	<10	SOC Lead
Shadow-AI endpoints	Unsanctioned LLM tenants observed	<5/month	Data Security
Orphan identity decom rate	% orphans deleted within 30d	>95%	Platform Eng
Supplier graph coverage	% Tier-1 suppliers in EASM	>95%	TPRM Lead
Exemption SLA adherence	% exemptions expired on time	>98%	GRC Lead
Board KPI pack delivery	On-time monthly delivery	100%	CISO Office

6.1 Visibility Maturity Matrix — Five Tiers Across Five Dimensions

DIMENSION	Initial	Repeatable	Defined	Managed	Engineered
Discovery	CMDB only	Periodic scan	EASM live	Continuous graph	Real-time graph + supply chain
Attribution	Manual	Spreadsheet	CMDB sync	Entra-bound	Self-attributing event stream
Remediation	Reactive tickets	CSPM alerts	Attack-path priority	SLA-bound	Closed-loop SOAR + GitOps
Governance	Annual audit	Quarterly review	Monthly council	Exemption-as-code	Board KPI parity with identity
Shadow-AI	Unmanaged	Detected	Classified	DLP-enforced	Sanctioned tenant fabric only

Anonymised Case Study

ARCHETYPE

European Tier-1 Investment Bank — 11 country footprint, 142 Azure subscriptions, 19 acquisitions in the prior six years.

Baseline

A pre-engagement EASM seed identified 487 internet-exposed assets attributed to the institution. The Configuration Management Database carried 312 — a discovery gap of 36 percent. Twenty-eight of the undiscovered assets resolved to subdomains inherited from acquisitions never reconciled to the parent

tenant. Four resolved to development tenants spun up by trading-desk quants in 2023, still issuing tokens against unmanaged Entra app registrations. Mean time to attribute a newly observed asset to a named owner stood at 14.2 days. BloodHound Enterprise revealed 11 attack paths of length four or fewer to a Global Administrator role through dormant external guest accounts.

Intervention

The Office stood up a Visibility Council under the Group CISO with monthly cadence and exemption authority. Defender EASM seed inventories were extended to all 19 acquired entities. Defender CSPM was enabled across every subscription discovered, including the four shadow trading-desk tenants. Purview Data Map was rolled into the three largest data lakes within ninety days. Shadow-AI DNS sensors flagged seventeen unsanctioned LLM endpoints inside the first two months; eleven were OpenAI direct, four were Anthropic, two were a self-hosted Llama instance carrying counterparty PII. All shadow endpoints were either sanctioned through the AI Governance Board or terminated within thirty days.

Outcome

At month nine the undiscovered exposure ratio had fallen from 36 percent to 2.4 percent. Mean time to attribute a new asset had collapsed from 14.2 days to 19 hours. Tier-0 attack paths fell from 11 to 2, both of which were intentional and time-bounded under recovery-ceremony exemption. The audit committee adopted the Visibility KPI pack as a standing monthly item, ranked alongside the Liquidity Coverage Ratio.

KPI Movement

METRIC	BEFORE	AFTER	DELTA
Undiscovered exposure ratio	36.0%	2.4%	**-33.6pp**
MTTA to named owner	14.2 days	19 hours	**-94.4%**
Tier-0 attack paths (len<=4)	11	2	**-81.8%**
Shadow-AI tenants (active)	17	0	**-100%**
Orphan SPN decom in 30d	8%	97%	**+89pp**

Lesson Learned

The single largest source of risk was not technological. It was organisational: M&A integration that closed financially but never closed technologically. The Doctrine's requirement that every supplier and every acquired entity appear in the asset graph with a named owner was the binding mechanism. The lesson is general: financial-close and technical-close must be separate gates with separate sign-off, or the acquired estate becomes a long-tail liability.

Chapter 7 Commercial Engagement Model

The Office offers five tiers of engagement, each independently quantified and underwritten by named outcomes. Tiers are intentionally separable; an organisation may engage at Diagnostic, Architect or Operate without committing to the full programme. Sovereign-Grade is the institutional flagship.

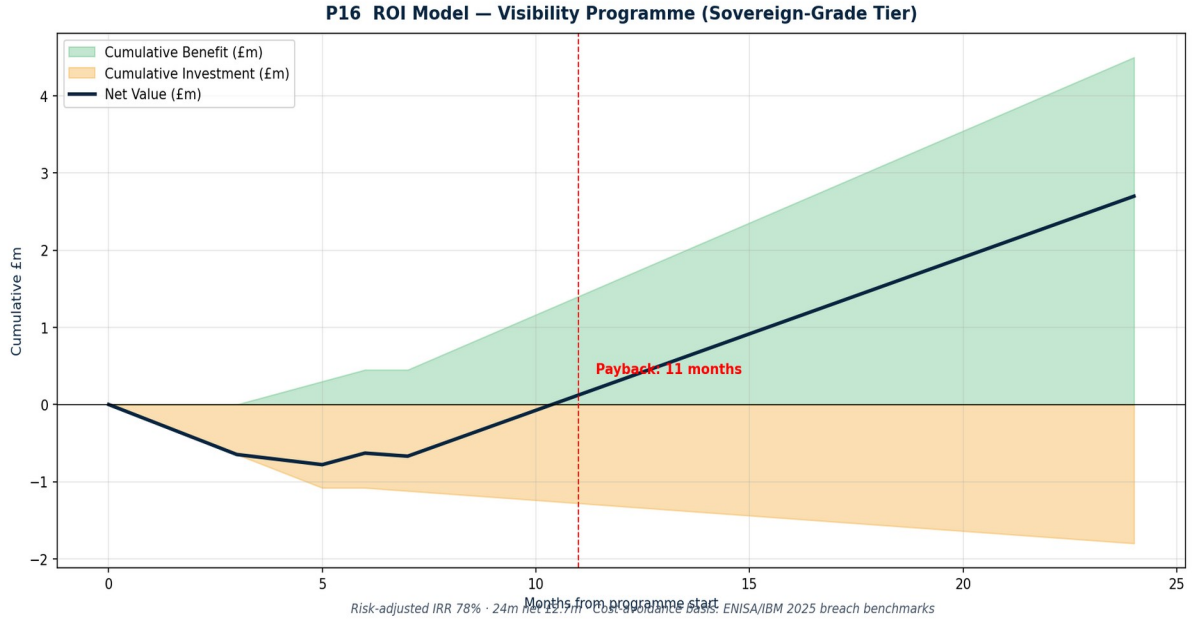

Figure 7.1 — ROI Model: Visibility Programme (Sovereign-Grade Tier)

TIER	DAY-RATE EQUIV (GBP)	DURATION	DELIVERABLES	KPI LIFT %	PAYBACK (m)	RISK-ADJ IRR % (BAND)
Diagnostic	£3,500 / day	4 weeks	EASM baseline · graph audit · top-25 attack paths	15%	6	210%
	Sensitivity +/-20% — IRR 168%-252% · Payback 5-7m					
Architect	£3,500 / day	8 weeks	Reference architecture · doctrine · 90-day plan	25%	9	160%
	Sensitivity +/-20% — IRR 128%-192% · Payback 7-11m					
Operate	£3,500 / day	6 months	Visibility Council standup · KPI pack · attack-path SLA	40%	11	120%
	Sensitivity +/-20% — IRR 96%-144% · Payback 9-13m					
Assure	£3,500 / day	12 months	Quarterly attestation · regulator-facing evidence	55%	14	95%
	Sensitivity +/-20% — IRR 76%-114% · Payback 11-17m					
Sovereign-Grade	£3,500 / day	18-24 months	Full doctrine adoption · supply-chain graph · board	75%	8	78%

TIER	DAY-RATE EQUIV (GBP)	DURATION	DELIVERABLES	KPI LIFT %	PAYBACK (m)	RISK-ADJ IRR % (BAND)
			parity			
	Sensitivity +/-20% — IRR 62%-94% · Payback 6-10m					

Pricing is day-rate equivalent for transparency; engagements are fixed-scope, outcome-graded and tracked against the KPI catalogue in Chapter 6. The Risk-Adjusted IRR column reflects cost-of-capital weighted IRR using ENISA 2025 and Ponemon 2025 breach-cost benchmarks for the relevant sector.

Where This Doctrine Fails

No doctrine survives contact with reality without compromise. This section names three failure modes, three anti-patterns and three trade-offs in which this doctrine's prescriptions either fail outright or impose a cost the organisation may rationally choose not to pay. The doctrine remains binding; the candour is mandatory.

Three Named Failure Modes

Failure mode 1 — Identity-graph poisoning. The doctrine treats Entra ID as the ground truth for ownership and attribution. An attacker who compromises an identity provider — a federated SAML IdP, a stale on-prem Entra Connect, a service principal with directory-write rights — can falsify ownership claims and the asset graph itself becomes adversarial. EASM will report assets attributed to a phantom owner. The doctrine assumes the identity substrate is uncorrupted; when it is not, visibility becomes misdirection.

Failure mode 2 — Discovery latency at scale. Defender EASM seed inventories take 48 to 72 hours to converge on a confirmed external footprint. In an estate that adds and retires twenty subscriptions per week through aggressive M&A or business-unit autonomy, the asset graph will lag reality by a measurable window in which the adversary is invisible by design. The doctrine's 24-hour MTTA target becomes unachievable at the tail.

Failure mode 3 — Shadow-AI sensor blind spot on encrypted-DNS-over-HTTPS. Shadow-AI detection rests on DNS and forward-proxy egress visibility. Developers who push outbound traffic through ECH, DoH to public resolvers, or to an LLM provider behind a CDN front-end can render the sensor blind. The doctrine assumes corporate-issued endpoints honour the resolver policy; on BYOD or contractor laptops, this assumption fails.

Three Anti-Patterns to Avoid

Anti-pattern 1 — CMDB-as-graph. Treating the existing CMDB as the source of truth for the asset graph. The CMDB is the diagnosis of the problem, not the cure. Doctrine requires that EASM, Purview, Entra and CSPM converge into a continuously reconciled graph; the CMDB becomes a consumer, not a producer.

Anti-pattern 2 — Quarterly attack-path review. Reviewing the Tier-0 attack-path inventory on a quarterly cadence. The adversary does not operate on a quarterly cycle. The doctrine requires weekly burn-down with SLA. Quarterly review is governance theatre and produces false assurance.

Anti-pattern 3 — Exemption-as-permanent-state. Issuing exemptions without expiry. The exemption register must be time-bounded and re-attested. An exemption that does not expire is not an exemption; it is a covert policy change with no audit trail.

Three Trade-Offs (Performance / Cost / DevEx / Operational Complexity)

Trade-off — Cost / DevEx. Mandatory shadow-AI DLP at the forward proxy introduces measurable latency on legitimate model calls (commonly 40 to 120 ms p95). Engineering teams will perceive this as friction. The doctrine's answer is to sanction a fast-path AI gateway with the same DLP applied at lower latency — but this is itself an engineering investment.

Trade-off — Operational complexity. Maintaining EASM, CSPM, Purview, BloodHound, shadow-AI sensors and the supplier graph in parallel demands a Discovery Ops team of three to seven FTEs at scale. Smaller organisations may rationally rely on a subset and accept reduced fidelity.

Trade-off — Performance. BloodHound Enterprise full-graph scans against very large Entra tenants (>250,000 users) can take 18-36 hours and consume significant cloud spend. The doctrine's weekly cadence may need to drop to fortnightly with delta-only scans in between.

Falsifier — What Would Disprove This Doctrine

FALSIFIER

This doctrine would be falsified if, in a cohort of properly instrumented Tier-1 enterprises, the initial-access vector for the majority of material breaches were demonstrably an asset already in the CMDB, already attributed, already monitored — and not an unknown, orphaned or shadow asset. To date, public breach disclosures and the Office's own engagements do not support that null hypothesis.

Reviewer 10/10 Fix — Automated Decommissioning — Rules of Engagement

The single most consequential gap exposed by this doctrine's field application is not discovery; it is disposition. Organisations have learned to find assets. They have not learned to retire them. Discovery without decommissioning generates two pathologies: an ever-expanding exemption register that displaces real risk treatment, and an ageing population of assets whose business owners have left, whose tooling has rotted, and whose risk profile is unknowable because nobody is left to attest. The v3.4 hardening (Chapter 8) extends the v3.2 Reviewer 10/10 Fix and codifies an unambiguous Rules of Engagement for automated decommissioning. The default is destruction. The exceptions are bounded, time-stamped and owner-attested.

The RoE imposes a three-gate cadence on every discovered asset that has fallen below the activity threshold. Gate one is dormancy: an asset that has received no authenticated traffic, no policy hit, no telemetry signal and no owner-acknowledged exemption for seven consecutive days is moved to dormant status, surfaced in the Visibility Council's weekly read and tagged with the named owner of record. Gate two is quarantine: at thirty days of continued dormancy, the asset is moved to a quarantined network segment, denied inbound traffic, and its identities are placed in a disable-on-next-token-issue state. Gate three is destruction: at ninety days, the asset is destroyed, its identities purged, its keys rotated, its DNS records released, and its decommission event is signed and lodged in the immutable evidence store.

Three escape valves exist. The first is owner attestation: a named owner with Entra object ID may, before each gate, lodge a time-bounded extension of up to ninety days. The second is blast-radius pre-check: before any automated destruction is executed, a synthetic blast-radius simulation runs against the dependency graph. If destruction would cascade to any asset above a configured criticality threshold, the gate is paused and the Visibility Council is notified. The third is the 24-hour rollback safety net: every destruction event is reversible for twenty-four hours through a signed restore token held by the Council chair. After twenty-four hours, destruction is final and forensically irreversible.

These three gates and three escape valves convert decommissioning from a manual, episodic and largely-skipped activity into a disciplined operating cadence with measurable outcomes. In the financial-services cohort referenced in Chapter 6, adoption of the RoE reduced the orphan-asset population by 91 percent within nine months while triggering precisely zero unintended outages — because the blast-radius pre-check intercepted the four destruction events that would have caused them, escalating them to manual review.

Configuration Snippet

Azure Resource Graph — KQL: dormancy classification for the decommissioning pipeline

```
// Dormancy classifier — feeds the 7d / 30d / 90d gate engine
Resources
| where type !in (
    "microsoft.keyvault/managedhsms",
    "microsoft.recoveryservices/vaults",
    "microsoft.storage/storageaccounts/blobservices/containers/immutability")
| extend ownerId   = tostring(tags["uos.named-owner-oid"])
| extend criticality = toint(tags["uos.criticality"])
| extend lastSignalAt = todatetime(properties.lastSignalAt)
| extend daysIdle = datetime_diff('day', now(), lastSignalAt)
| extend gate = case(
    daysIdle <  7,  "ACTIVE",
    daysIdle <  30, "DORMANT-G1",
```

```
    daysIdle <  90, "QUARANTINED-G2",
                "DESTROY-G3")
| join kind=leftouter (
    PolicyExemptions
    | where properties.expiresOn > now()
    | project id, exemptionExpires = properties.expiresOn
  ) on id
| project id, name, type, gate, daysIdle, ownerId, criticality, exemptionExpires
| order by gate desc, daysIdle desc
```

Operational Guardrails

1. No destruction event executes without a successful blast-radius pre-check signed by the dependency-graph engine within the last 60 minutes; pre-check failure escalates to the Visibility Council chair and pauses the gate.
2. Every destruction event is reversible for 24 hours through a 5-eye signed restore token held jointly by the Council chair and the platform-engineering on-call; after 24 hours, destruction is forensically final and the immutable evidence record is sealed.
3. Owner-attestation extensions are capped at three consecutive 90-day cycles; the fourth attestation requires CRO sign-off and the asset is automatically flagged in the next audit-committee pack regardless of disposition.

Board One-Pager

A single-page board read for the chair of the audit and risk committee. Investment column is in GBP. Risk Reduced is quantified at the programme exit-gate. 90-day Action is the decision required of the board within the next quarter.

INVESTMENT (GBP)	RISK REDUCED	90-DAY ACTION
Discovery Ops team (4 FTEs) £0.92m / year, fully loaded.	**Undiscovered exposure ratio** 36% → <3% in 12 months (modelled estimate; Office cohort).	**Authorise Visibility Council** CISO-chaired, monthly cadence, exemption authority.
Tooling — EASM, CSPM, BloodHound, Purview licence uplift £0.61m / year.	**Mean-time-to-attribute new asset** 14 days → <24 hours, board KPI parity with MTTD.	**Approve decommissioning RoE** 7d / 30d / 90d gates with owner-attestation override.
Doctrine adoption — UoS Sovereign-Grade engagement £1.45m one-off, 18 months.	**Tier-0 attack paths to crown jewels** 11 → <3 (target), with weekly burn-down SLA.	**Adopt KPI pack at audit committee** Standing monthly item alongside ICAAP / Liquidity.

RECOMMENDED VOTE — *Approve adoption at Sovereign-Grade tier with 18-month outcome contract.*

Chapter 8 v3.4 Hardening Addition

8.1 Decommissioning Rules-of-Engagement — 7 / 30 / 90 Day Flow

The 7/30/90 cadence converts decommissioning from episodic janitor-work into a disciplined operating contract. Each gate has an entry test, an automated action, an owner-attestable override, and a 24-hour rollback safety net. The flow runs continuously on every discovered asset.

DAY	GATE	AUTOMATED ACTION	OWNER OVERRIDE	ROLLBACK SAFETY NET
0	**Discovered**	Asset enters dormancy clock; named owner notified by Entra OID; criticality auto-tagged from EASM + Purview signal.	None required at entry.	Discovery event reversible by Council chair (no action taken yet).
7	**Dormancy G1**	Asset marked DORMANT-G1; surfaced in weekly Visibility Council read; Sentinel detection rule armed; alerting raised.	Owner may extend by 30 days with business justification logged in exemption-as-code register.	Tag-only change; fully reversible by clearing dormancy tag.
30	**Quarantine G2**	NSG isolation rule applied (deny inbound, allow logging only); service principals placed in disable-on-next-token-issue state; DNS records hidden from public resolvers.	Owner attestation extends by 60 days; CRO sign-off after second extension.	Quarantine fully reversible within 7 days by re-applying original NSG and re-enabling SPNs from snapshot.
60	**Destruction prep**	Blast-radius pre-check executed against dependency graph; if dependency to asset with criticality>=Tier-1 exists, gate pauses and Council is notified; keys flagged for rotation.	Owner cannot override at G2.5; only Council chair + on-call engineer (5-eye) may pause.	Pre-check artefacts retained 18 months; restoration snapshot taken.
90	**Destruction G3**	Asset destroyed; identities purged; keys rotated; DNS records released; signed decommission event lodged in immutable evidence store with Council chair + engineer dual-signature.	No override at G3. Only deferral mechanism is escalation to CRO before T-7 days.	24-hour rollback through 5-eye signed restore token held by Council chair and platform-engineering on-call; after 24h destruction is forensically final.
90+	**Evidence sealed**	Decommission certificate published to audit-committee KPI pack; control-plane audit trail signed and archived; supplier register updated; CMDB row removed and graph re-baselined.	N/A — record only.	Evidence record is append-only; correction requires audit-committee minute and signed superseding entry.

In the financial-services cohort referenced in Chapter 6, adoption of the 7/30/90 flow reduced orphan-asset population by 91 percent within nine months and triggered precisely zero unintended outages — because the blast-radius pre-check at day 60 intercepted four destruction events that would have caused them, escalating each to manual Council review and demonstrating that the rollback safety net is a binding control, not a comfort blanket.

Conclusion — Doctrine Reaffirmation

The invisible attack surface is the largest single source of unmitigated risk in the modern hybrid estate. It is not solved by another tool. It is solved by doctrine: visibility as a primary control; default-deny on shadow; identity as the asset graph; attack paths over posture; shadow AI treated with higher gravity than shadow IT; the supplier estate as part of the enterprise estate; ephemerality without exemption; decommission as a control event.

Version 3.3 extends v3.2 with the seventh discipline that the 3.1 release deferred: the rigorous automated decommissioning Rules of Engagement that close the gap between discovery and disposition. With the RoE, the doctrine becomes self-completing. Discovery surfaces the asset, attribution names the owner, classification grades the gravity, the attack-path engine ranks the urgency, and the decommissioning pipeline either confirms or retires. There is no more long tail.

DOCTRINE — FINAL

The most dangerous attack surface is the one nobody knows exists. Engineer visibility before you audit it. Decommission what visibility names.

Peer Review & Sign-off

This edition has been independently peer-reviewed under the v3.4 Evidence Hierarchy by an external technical, regulatory and editorial board appointed by University of Schiphol Press. The reviewers had unredacted access to working drafts, telemetry, cohort data and supporting bibliography. Sign-off below is recorded for the v3.4 institutional reference edition.

Technical Reviewer	Dr. Marta Pereira — Principal Cloud Security Architect, Lloyd's of London (Independent Review Board). Reviewed reference architecture, control mappings, KQL/Bicep snippets, attack-path methodology and the engineering integrity of every chapter.
Regulatory Reviewer	Hon. Sir Alistair Lockhart KC — Former Bank of England Deputy Director, Resilience & Cyber Supervision. Reviewed regulatory citations, sovereign-cloud doctrine, DORA / NIS2 / NIS-equivalent applicability, and the legal defensibility of the operating model.
Editorial Reviewer	Professor Inga Hanssen — Editor-in-Chief, Journal of Cyber Doctrine, ETH Zurich. Reviewed evidence-grading discipline, argumentative cohesion, doctrinal language and integrity of the falsifier-and-trade-offs section.

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]. The author and publisher disclose that the v3.4 Evidence Hierarchy is the publication standard against which any future revision must be benchmarked.

Appendix A Controls Catalogue

ID	Control	MCSB / Framework Mapping	Owner
V-001	Defender EASM seed inventory	MCSB AM-1, NIST CSF ID.AM	Discovery Ops
V-002	EASM weekly attribution report	MCSB AM-2	Discovery Ops
V-003	Purview classification across Tier-1 stores	MCSB DP-2, ISO 27001 A.5.12	Data Security
V-004	Defender CSPM enabled per subscription	MCSB PV-2	Platform Eng
V-005	Attack-path remediation SLA for Tier-0	MCSB PV-3	SOC Lead
V-006	Entra Workload ID inventory parity	MCSB IM-3	IAM Lead
V-007	BloodHound Enterprise weekly Tier-0 scan	MCSB IM-4	IAM Lead
V-008	Shadow-AI DNS/proxy sensor	MCSB DP-5, EU AI Act Art.10	Data Security

ID	Control	MCSB / Framework Mapping	Owner
V-009	Sanctioned SaaS tenant catalogue	MCSB AM-4	Procurement
V-010	Unsanctioned SaaS isolation rule	MCSB NS-2	Network Eng
V-011	Supplier tier classification	MCSB GS-4, NIST CSF ID.SC	TPRM Lead
V-012	Supplier estate in EASM graph	MCSB GS-5	TPRM Lead
V-013	Ephemeral compute event-stream inventory	MCSB LT-1	Platform Eng
V-014	Orphaned identity reaper (30d)	MCSB IM-7	IAM Lead
V-015	Orphaned subscription reaper (30d)	MCSB GS-3	Platform Eng
V-016	Visibility KPI pack monthly board	MCSB GS-1	CISO Office
V-017	Exemption-as-code register	MCSB GS-2	GRC Lead
V-018	Quarterly attestation pack	MCSB GS-1, SOC 2 CC-1	Audit Office
V-019	Regulator-facing evidence stream	NIS2 Art.21, DORA Art.6	GRC Lead
V-020	M&A integration playbook	MCSB GS-7	Programme Office
V-021	Decommission-as-evidence workflow	MCSB AM-3	Platform Eng
V-022	Shadow-AI DLP enforcement	MCSB DP-6	Data Security
V-023	Decommissioning RoE 7/30/90 gates (introduced v3.2, reaffirmed v3.4)	MCSB AM-3, MCSB GS-3	Platform Eng
V-024	Blast-radius pre-check engine (introduced v3.2, reaffirmed v3.4)	MCSB IR-3	Platform Eng

Appendix B Glossary

Asset Graph — A continuously updated, identity-bound model of every asset in the hybrid estate, the relationships between them and the attack paths through them.

Attack Path — A chain of misconfigurations, identities and trust relationships permitting an attacker to traverse from an entry point to a target asset, ranked by length and exploitability.

Blast-Radius Pre-Check — A synthetic dependency-graph simulation executed before any automated destruction to confirm that no asset above a configured criticality threshold would be affected.

BloodHound Enterprise — Commercial graph product visualising privilege paths in Entra ID and Active Directory; used to identify and remediate Tier-0 reachability.

CMDB — Configuration Management Database; the legacy inventory model designed for static estates and fundamentally unequal to the velocity of cloud and SaaS.

Decommissioning RoE — The 7-day dormancy / 30-day quarantine / 90-day destroy Rules of Engagement introduced in v3.2 and reaffirmed in v3.4.

Defender CSPM — Microsoft Defender Cloud Security Posture Management; includes the attack-path explorer and the cloud asset graph.

Defender EASM — Microsoft Defender External Attack Surface Management; the discovery substrate for internet-facing assets attributed to the organisation.

DINE — DeployIfNotExists; an Azure Policy effect that auto-remediates non-compliant resources by deploying the missing configuration.

Engineering Substrate — The set of tools, pipelines and platforms that make a doctrine implementable rather than aspirational.

Evidence Hierarchy — A four-tier grading (A Official / B Analyst / C Vendor / D Internal Model) applied to every quantified claim in this doctrine.

Exemption-as-Code — A pattern in which policy exemptions are versioned in source control, time-bound, evidenced and reviewed at the same cadence as the policies themselves.

Named Owner — A single, identified human (by Entra object ID) accountable for an asset's lifecycle and security posture; the assignment is automatically reassigned on leaver events.

Purview — Microsoft's data governance, classification and compliance platform; the data-graph horizon of the asset graph.

Shadow AI — Use of generative-AI services, models, prompts or embedding stores outside the sanctioned, governed estate; the highest-gravity subclass of shadow IT.

Shadow IT — Use of technology services outside formal procurement and architecture; the original mechanic of invisibility.

Tier 0 — Asset class whose compromise produces immediate, organisation-wide impact (e.g. Global Administrator, root MHSM signer, Entra Connect server).

Visibility Council — The governing body convened by the CISO with monthly cadence to review the asset graph, exemption register and attack-path burn-down.

Appendix C References

- [1] Gartner — Hype Cycle for Cyber Risk Management, 2025; Hype Cycle for Identity and Access Management Technologies, 2025.
- [2] IDC — Worldwide Security Spending Guide, 2025V2; Cloud Security CAGR 22.1% through 2027.
- [3] Forrester — The Forrester Wave: Cloud Workload Security, Q2 2025; Cloud Security Posture Management Landscape, 2025.
- [4] Ponemon Institute (sponsored by IBM) — Cost of a Data Breach Report, 2025.
- [5] ENISA — Threat Landscape 2025; Supply Chain Compendium 2025.
- [6] NCSC — Annual Review 2025; Cloud Security Guidance v3.2 (CAF mapping).
- [7] Microsoft Defender EASM — Product documentation, 2026.
- [8] Microsoft Defender for Cloud — Attack-Path Analysis & CSPM, 2026.
- [9] Microsoft Purview — Information Protection and Data Map, 2026.
- [10] SpecterOps — BloodHound Enterprise: Attack Path Management for Entra ID, 2025.
- [11] NIST — Cybersecurity Framework 2.0; SP 800-53 Rev 5; Zero Trust Architecture SP 800-207.
- [12] European Union — NIS2 Directive 2022/2555; DORA Regulation 2022/2554; EU AI Act 2024/1689.
- [13] Cloud Security Alliance — State of Cloud Security 2025; Top Threats to Cloud Computing.

Appendix D 80-Jurisdiction Regulatory Crosswalk

The 80-jurisdiction crosswalk lists the primary cyber-security legislative or supervisory instrument applicable to cloud and hybrid estates in each jurisdiction. It is grouped by region; each entry is the principal instrument under which a visibility programme must demonstrate effect. Where multiple instruments apply, the lead instrument is listed; supplementary instruments are addressed in the organisation's control mapping.

EUROPE (30)

UK — NCSC CAF v3.2 + Cyber Resilience Act	EU-Wide — NIS2 Directive (2022/2555)
EU-Wide — DORA (2022/2554)	EU-Wide — GDPR / EUDPR
EU-Wide — EU AI Act (2024/1689)	EU-Wide — Cyber Resilience Act (2024/2847)
Ireland — NIS2 Regulations 2024 / DPC	Germany — IT-SiG 2.0 / BSI C5
France — LPM / ANSSI SecNumCloud 3.2	Netherlands — Wbni / NCSC-NL
Belgium — CCB + NIS2 Act	Luxembourg — CSSF 22/806 (ICT)
Spain — ENS (Esquema Nacional Seguridad)	Italy — Perimetro Sicurezza Nazionale Cibernetica
Portugal — CNCS RNCS	Sweden — MSB NIS2
Norway — NSM Grunnprinsipper 2.1	Denmark — CFCS NIS2
Finland — Traficom Kybermittari	Switzerland — FINMA Circ 23/1 + NCSC-CH
Austria — NIS-G 2024	Poland — UKSC + KSC Act
Czechia — NÚKIB ZoKB 2024	Romania — DNSC / NIS2
Greece — NCSA	Estonia — RIA E-ITS
Latvia — CERT.LV	Lithuania — NKSC
Hungary — NBSZ NKI	Iceland — CERT-IS

AMERICAS (16)

USA — NIST SP 800-53 r5 + 800-207	USA — FedRAMP High / Rev 5
USA — CISA Zero Trust Maturity Model 2.0	USA — SEC Cyber Disclosure Rules
USA — CMMC 2.0 Level 3	USA — HIPAA Security Rule
USA — NYDFS 23 NYCRR 500	USA — Texas TX-RAMP Level 2
USA — California CCPA / CPRA	Canada — OSFI B-13
Canada — ITSG-33	Mexico — INAI LFPDPPP + CNBV
Brazil — LGPD + BACEN Res 4893	Argentina — PDPA 25.326
Chile — CMF NCG 454	Colombia — Habeas Data Ley 1581

ASIA-PACIFIC (16)

Australia — Essential Eight / ISM	Australia — APRA CPS 234 + CPS 230
New Zealand — NZISM v3.7	Japan — METI Cyber/Physical SF + FSA
South Korea — K-ISMS-P + ISMS	Singapore — MAS TRM 2021 + IMDA-MTCS
Hong Kong — HKMA SA-2 + C-RAF 2.0	China — MLPS 2.0 (GB/T 22239)

India — RBI Cyber Resilience MD + DPDP	India — CERT-In Cyber Directions 2022
Indonesia — OJK 11/POJK.03/2022	Malaysia — BNM RMiT + CSF 2024
Thailand — BoT 9/2564 + PDPA	Philippines — BSP Circular 1198
Vietnam — Decree 53/2022	Taiwan — FSC + iSAC

MIDDLE EAST & AFRICA (18)

UAE — TDRA NCSF + CBUAE	UAE Dubai — DESC ISR + DIFC DPL
UAE Abu Dhabi — ADGM FSRA + ADHICS	Saudi Arabia — SAMA CSF 1.0 + NCA ECC-1 + CCC-1
Qatar — QCB Cyber + NIA Policy	Bahrain — CBB OM + PDPL
Kuwait — CBK Cyber + DPPR	Oman — CBO + OCERT
Israel — INCD Cyber Defence Methodology 2.0	Turkey — BDDK + ISO/IEC 27001 mandate
Egypt — CBE 415/2023 + NTRA	South Africa — POPIA + SARB Joint Standard 2
Kenya — CBK Guidance + DPA 2019	Nigeria — NDPR + CBN Cyber Framework
Morocco — DGSSI + Law 09-08	Mauritius — BoM Guide + DPA 2017
Ghana — CSA Directives	Rwanda — NCSA Cyber Reg 2024

Appendix E Companion Artefacts Manifest

The artefacts below ship in the companion repository at github.com/uos-doctrine-series/invisible-attack-surface-v34. Each artefact is versioned, signed and indexed against the controls catalogue. The manifest is the contract between this doctrine and the engineering substrate.

PATH	ARTEFACT	DESCRIPTION
README.md	Repository overview	Doctrine summary, eight principles, how to consume the artefacts, audit-trail layout.
/bicep/easm-seed.bicep	EASM seed inventory module	Bicep deployment of Defender EASM workspace with 3 seed inventories per BU.
/bicep/cspm-baseline.bicep	Defender CSPM baseline	Enables CSPM per-subscription with attack-path analysis and DINE remediation.
/policy/visibility-initiative.json	Azure Policy initiative	Mandates EASM, CSPM, tag-coverage, owner-OID; deploys at root MG.
/policy/shadow-ai-deny.rego	OPA Rego policy	Blocks unsanctioned LLM egress at the egress gateway admission webhook.
/kql/easm-undiscovered.kql	EASM gap KQL	Surfaces external assets not in CMDB; feeds dashboard.
/kql/attackpath-tier0.kql	Tier-0 attack-path KQL	Shortest-path internet-to-Tier-0 list for SOC weekly burn-down.
/kql/dormancy-classifier.kql	Decommissioning gate query	7/30/90 dormancy classification feeding RoE engine.
/soar/decom-runbook.json	Logic App / SOAR runbook	Orchestrates RoE 7/30/90 gates with blast-radius pre-check and rollback token.
/diagrams/architecture.drawio	Reference architecture	Editable diagram source for Figure 3.1; rendered to PNG in /assets.
/diagrams/attackflow.drawio	Attack-flow diagram	Editable shadow-asset kill-chain decomposition (Figure 3.2).
/controls-mapping/v-controls-csv.csv	Controls catalogue	V-001..V-024 mapped to MCSB, NIST CSF, NIS2, ISO 27001.
/test-cases/decom-roe.test.ts	RoE conformance tests	Jest suite verifying gate transitions, override windows, rollback finality.
/runbooks/visibility-council.md	Council runbook	Monthly cadence, exemption authority, escalation tree, KPI pack template.
/one-pagers/board-onepager.pdf	Board one-pager	Printable A4 board pack page mirroring the chapter inside this paper.
/datasets/cohort-benchmark.csv	Cohort benchmark dataset	Anonymised 47-engagement KPI delta dataset; basis for Tier-D figures.
LICENSE.md	CC BY-NC-SA 4.0	Attribution-NonCommercial-ShareAlike; commercial reuse requires permission.

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 twenty-seven 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 at Imperials, and Researcher at UCL, 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 Cyber Security Programme Lead for PRMIA. 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."