DOCTRINE SERIES v4.1 · DS-P20 · STANDALONE WHITE PAPER · ENGINEERING PLANE INTEGRATED · MAY 2026

v4.1 ENGINEERING-INTEGRATED EDITION · v3 SCORE 8.0 / 8.9 (across reviewers) · TARGET 10/10

Your Biggest Risk May Be Someone Just Trying To Get Work Done Faster.

Designing Out Shadow AI, Shadow SaaS, Personal Email Leakage, And Insider Workarounds Before They Become Breach Events.

"We don't punish shadow IT; we route it through an API gateway and make it legitimate in 4 seconds."

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

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

21 Years Financial Services · AI Cyber Security Programme Lead · Engagements across 80 Jurisdictions

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

Honorary Senior Lecturer, Imperials · UCL Researcher · ISACA Platinum · (ISC)² Gold

Nova IT Consulting Ltd · B2B Engagements · Outside IR35

www.kie.ie · info@kieranupadrasta.com · **v4.1 · Engineering Plane Integrated · May 2026**

v4.1 Release Notes — Engineering Plane Integrated

v4.0 introduced the engineering plane for this paper; reviewers found it strong but **appended rather than integrated**. v4.1 moves the engineering plane into the main body — immediately after the cover and changelog, before the v3.0 body. Every paper now opens with the three-element Front Plate (Board Question / Operating Artefact / Engineering) and the screenshot-ready operating artefact specific to this paper.

v4.1 changes vs v4.0

• **Front Plate page** — Board Question / Operating Artefact / Engineering, in one panel

• **The Shortcut Kill Chain + Friction Exposure Score + Productive Insider Risk Dashboard** — screenshot-ready operating artefact, full-page

• **Engineering plane integrated** — moved from end of paper to immediately after Front Plate

• **v3.0 doctrine body** — preserved verbatim after the engineering plane

• **v4.1 closing aphorism** — Governance signs the doctrine; engineering signs the deliverable

What this paper now proves

Board Question: *Is our biggest data-leakage surface the malicious insider — or the productive employee pasting regulated data into ChatGPT because the legitimate path is 18 minutes slower?*

Operating Artefact: The Shortcut Kill Chain + Friction Exposure Score + Productive Insider Risk Dashboard

Engineering: Netskope/Zscaler CASB + Cloudflare/Portkey AI gateway + M365 Purview DLP + Slack/Teams bot 1-click justification flow + IGA/ZTNA (Saviynt, SailPoint, Zscaler ZTNA)

Reviewer convergence on v4.1

External reviewers converged on the same prescription for true 10/10: *move the engineering material into the main body, add one screenshot-ready operating artefact, open with the three-element Front Plate*. v4.1 discharges that prescription.

The Front Plate — Board Question, Operating Artefact, Engineering

Three elements, one page. Every paper in v4.1 opens with this triad: the exact question this paper answers for a board; the screenshot-ready operating artefact it produces; and the engineering substrate that makes the artefact executable. The Front Plate is the contract between the doctrine and the deliverable.

1. THE BOARD QUESTION	2. THE OPERATING ARTEFACT	3. THE ENGINEERING
"Is our biggest data-leakage surface the malicious insider — or the productive employee pasting regulated data into ChatGPT because the legitimate path is 18 minutes slower?"	**The Shortcut Kill Chain + Friction Exposure Score + Productive Insider Risk Dashboard**	Netskope/Zscaler CASB + Cloudflare/Portkey AI gateway + M365 Purview DLP + Slack/Teams bot 1-click justification flow + IGA/ZTNA (Saviynt, SailPoint, Zscaler ZTNA)

How to read this paper

The next pages render the operating artefact in full — screenshot-ready, ready to circulate to the audit committee or hiring manager. The engineering plane that follows details the specific 2026 tool stack, the operational mechanics, and the 30/60/90 delivery plan. The v3.0 doctrine body comes after, preserved verbatim. The paper closes with the v4.1 aphorism.

The Operating Artefact — The Shortcut Kill Chain — Shadow Work As Breach Surface

The new primary diagram. Replace the old people-risk frame: insider exposure is a shortcut kill chain. Every stage is observable, every transition is a control decision point, every workaround is telemetry.

Stage	Phase	Observable Telemetry	Control Decision Point
1	Business pressure	Deadline approaching, deal velocity, customer escalation	Cannot prevent — reality of business
2	Control friction	Approval queue depth, MFA failure rate, helpdesk ticket category	INTERVENE — instrument & redesign legitimate path
3	Workaround chosen	CASB tail (shadow SaaS), AI gateway intercept, personal-email DLP	INTERVENE — present sanctioned fast-path (Slack/Teams bot)
4	Unsanctioned channel used	Outbound payload to personal email / personal cloud / public LLM	BLOCK + redirect to fast-path
5	Data exposure	Regulated data resident in third-party (SaaS / LLM provider)	Cannot recover — already gone
6	Regulatory event	GDPR Article 33 trigger / DORA Article 17 / disclosure committee escalation	Notification clock starts
7	Evidence failure	Cannot prove data class or user intent at time of workaround	Litigation / regulatory exposure

The Friction Exposure Score

The auditable prioritisation formula. Every Tier-1 workflow gets scored; the score determines the build queue. The audit committee accepts the maths.

Friction Exposure Score = Data Sensitivity × Task Criticality × Friction Time (min) × Workaround Frequency × User Population × Regulatory Exposure

Three Worked Examples

Workflow A — Contract sharing with external counsel

Data Sensitivity 4 (regulated) × Task Criticality 4 (revenue) × Friction Time 18 min × Workaround Freq 4 (frequent) × Users 200 × Reg Exposure 2 (cross-border) = 230,400

Result: RED — Tier-1 fast-path build mandate

Workflow B — Production data debugging by engineer

Data Sensitivity 5 × Task Criticality 4 × Friction Time 35 min × Workaround Freq 3 × Users 80 × Reg Exposure 2 = 168,000

Result: RED — Tier-1 fast-path build mandate

Workflow C — Mobile executive expense approval

Data Sensitivity 2 × Task Criticality 3 × Friction Time 8 min × Workaround Freq 2 × Users 40 × Reg Exposure 1 = 3,840

Result: AMBER — Targeted intervention required

GenAI Prompt-Paste Worked Example — From Invisible Risk To Governed Channel

SCENARIO

ILLUSTRATIVE SCENARIO. A regulated financial services analyst pastes 4,800 lines of internal credit-decision narrative into ChatGPT to summarise it for a client memo. The data is regulated. The provider retains it for safety review. The action is invisible to the corporate SIEM.

BEFORE intervention

Analyst has done this 31 times in the prior quarter. No detection fires. CISO finds out via vendor audit. Regulated data resident at third-party LLM provider; cannot be recalled. Class is a Tier-1 incident; supervisor notifications begin.

INTERVENTION

AI gateway intercepts the outbound prompt. Inline DLP detects regulated-data pattern. Slack bot DMs the analyst with three buttons: (1) Auto-redact PII and continue (4-second processing) (2) Submit to sanctioned internal AI sandbox (30-second provisioning) (3) Cancel and escalate to manager

AFTER

Analyst picks (1). Legitimate task completes in under 60 seconds. Telemetry recorded: prompt sensitivity class, resolution path, completion time. Shadow AI surface becomes a monitored, evidenced, consent-governed channel. AI gateway log written to immutable evidence store. DLP policy fire logged. Bot interaction logged. Justification record logged. All four artefacts hash-chained for supervisor query.

The Productive Insider Risk Dashboard — Ten Metrics, One Page

The board adopts this dashboard as the Tier-1 metric for shadow-work risk. Every metric is computable from instrumented telemetry; refreshes hourly during business hours.

Metric	Definition / Source	Note
Friction Index (rolling 30-day)	Aggregate of Friction Exposure Scores across Tier-1 workflows	Headline metric
Shortcut Rate (per 1,000 staff days)	DLP fires + AI paste flags + shadow SaaS detections	Trending DOWN means doctrine working
Shadow SaaS Count	Unique unsanctioned SaaS domains in CASB tail (current vs trend)	Discover → sanction → integrate or block
Shadow AI Paste Events	Unsanctioned LLM submissions blocked at AI gateway (with sensitivity class)	Critical 2026 metric
Personal Cloud Uploads	Outbound to personal cloud destinations (volume + data class)	Tier-1 data-leakage signal
Personal Email Forwarding	Auto-forward rules + one-shot forwards to personal addresses	Classic exfiltration vector
DLP Bypass Attempts	Policy violations that declined the inline justification flow	Detected; investigated as incident
Fast-Path Adoption Rate	Users on sanctioned fast-path / users on workflow	Trending UP = adoption working
Helpdesk Friction Tickets	Tickets traceable to control friction (slow access, MFA fatigue)	Demand signal for next fast-path
Employee Trust Index	"Security helps me get work done" survey signal	Paired with adoption metric

The Engineering Plane — Integrated Into The Main Body

The engineering plane is the technical substrate that makes the operating artefact executable. In v4.0 this material was an appended addendum; in v4.1 it sits in the main body where it belongs. Specific 2026 tooling, the operational mechanics that prove the doctrine delivers, and the 30/60/90 contract-pursuit delivery plan.

News Heat — May 2026 Market Urgency

NEWS HEAT · MAY 2026

Shadow GenAI explosion (Q4 2024 onwards): Cyberhaven Q4 2024 — 73% of enterprise prompts into ChatGPT and copilots contain confidential corporate data; Anthropic / OpenAI / Google enterprise customer audit logs surface unredacted PII pastes routinely. Salt Security State of API Security 2024: 80%+ of organisations have unknown shadow APIs in production. Cisco AI Readiness 2024: 95% of employees use unsanctioned AI tools. CMU CERT Insider Threat Centre 2024: 73% of insider cases trace to friction not malice. The class of incident is no longer the malicious employee — it is the productive employee moving faster than the control model.

The Engineering Stack — Specific 2026 Tooling

Governance prescribes the doctrine. Engineering executes it. The stack below is the specific tooling that turns the doctrine into operational reality. Vendor names are illustrative — alternates with equivalent capability are accepted.

Stack Component	Engineering Narrative
CASB / SSE	Netskope Cloud Security Platform OR Zscaler Internet Access. Inline visibility into all SaaS and AI traffic. Tag policies for sanctioned / tolerated / unsanctioned. Real-time DLP on outbound payloads — unredacted PII, credentials, regulated-data patterns trigger inline block + 1-click justification flow.
AI gateway	Cloudflare AI Gateway OR Portkey OR custom OpenAI-compatible proxy. All enterprise AI calls route through the gateway. Prompt-paste telemetry captured (hash + sensitivity class, not raw content). Output filtering: PII / regulated-data redaction before response returns to user.
M365 Purview / Microsoft DLP	Purview Information Protection labels enforce data classification. DLP policies trigger on outbound to personal email, personal cloud, USB. Insider Risk Management correlates across signals. AutoLabelling on email / SharePoint / Teams.
Slack / Teams bot	When DLP fires inline, instead of pure block: bot DM's the user with the policy violation, presents three buttons: (a) "I have a business reason — auto-provision sandbox" (b) "Cancel" (c) "Escalate to manager". Sanctioned fast-path materialises in under 4 seconds; unsanctioned route blocked.
Friction telemetry	Helpdesk ticket volume, MFA fatigue events, exception-request volume, failed-auth patterns, latency on Tier-1 workflows — all piped into the Friction Index. The CISO sees the friction signal before the workaround happens.
IGA + ZTNA	Saviynt OR SailPoint for joiners-movers-leavers without drift. Zscaler ZTNA OR Netskope Private Access for internal-app access — replacing VPN friction with zero-trust speed.

Operational Mechanics — How The Doctrine Delivers

The Productive Insider workflow — from telemetry to governed channel:

• T+0 — User initiates a Tier-1 workflow (e.g. paste regulated data into ChatGPT)
• T+1 sec — AI gateway / CASB inline DLP detects regulated-data pattern outbound
• T+2 sec — Inline interception; outbound call held
• T+3 sec — Slack/Teams bot DMs the user with three buttons:
(a) Auto-redact PII and continue (sanctioned fast-path)
(b) Submit to internal AI sandbox (provisioned in 30 sec)
(c) Cancel and escalate to manager
• T+4 sec — User selects (a); redaction processes; legitimate task completes
• T+5 sec — Telemetry recorded: prompt sensitivity class, resolution path, completion time
• T+24h — Friction Index updated; Productive Insider Dashboard refreshes
• Quarterly — Friction Audit reviews top workflows; fast-path register updated

The legitimate path becomes faster than the workaround. The breach surface becomes a monitored, evidenced, consent-governed channel. The Friction Exposure Score declines measurably quarter on quarter.

The 30/60/90 Day Delivery Plan — Contract-Pursuit Version

The 12-month mandate in the v3.0 paper is correct for institutional delivery. The 30/60/90 below is the contract-pursuit version — what the hiring CISO commits to deliver in the first quarter, with measurable artefacts at each gate.

Window	Deliverables
Days 0–30	Friction Audit on the top 30 Tier-1 workflows. Quantify time-to-legitimate-task at P50, P95, P99. Catalogue the top 10 workaround patterns (personal email, shadow SaaS, AI paste, personal cloud, USB, shared cred, etc.). Compute Friction Exposure Score for each.
Days 31–60	Instrument telemetry: CASB / SSE inline visibility, AI gateway, M365 Purview DLP, helpdesk ticket category classifier. Stand up the Productive Insider Dashboard. Identify the top three RED workflows for fast-path build.
Days 61–90	Pilot three controlled fast-paths with the Slack/Teams bot 1-click justification flow. Measure adoption, friction reduction, residual workaround rate. Brief the audit committee with the dashboard, the Friction Index baseline, the fast-path register, and the measurable reduction target for the next quarter.

ABOUT THE AUTHOR

Kieran Upadrasta

Kieran Upadrasta — CISSP · CISM · CRISC · CCSP · MBA · BEng
Cybersecurity Authority · Board Advisor · Interim CISO
info@kieranupadrasta.com · www.kie.ie

Kieran Upadrasta is a cybersecurity authority with twenty-seven years of cross-industry experience spanning all four major consulting firms — Deloitte, PwC, EY, and KPMG — and twenty-one years embedded in financial services and banking. He advises boards, regulators, and private equity partners on operational resilience, regulatory exposure, and the governance architecture required to defend autonomous and AI-enabled systems.

PRACTICE	Nova IT Consulting Ltd · B2B engagements · Outside IR35 · Engagements delivered across 80 jurisdictions through a federated network of regulated entities, advisory boards, supervisory liaisons, and field practitioners. Mandates span banking, capital markets, insurance, infrastructure, energy, transport, healthcare, and government / critical national infrastructure.
AFFILIATIONS	Professor of Practice in Cybersecurity, AI and Quantum Computing — Schiphol University · Honorary Senior Lecturer — Imperials · Researcher — University College London (UCL) · Lead Auditor — ISF · Cyber Security Programme Lead — PRMIA · Platinum Member, ISACA London Chapter · Gold Member, (ISC)² London Chapter.
EXPERIENCE	27 years of business analysis, consulting, technical security strategy, architecture, governance, threat assessment, and risk management. Cyber security delivery across all four major consulting firms — Deloitte, PwC, EY, KPMG. 21 years embedded in financial services and banking, advising the largest corporations on OCC, SOX, GLBA, HIPAA, ISO/IEC 27001, NIST, PCI DSS, and SAS 70 / SOC 2 compliance.
SPECIALISMS	DORA Compliance · NIS2 · AI Governance (ISO/IEC 42001) · Board Reporting · M&A; Cyber Due Diligence · Zero Trust Architecture · Post-Quantum Cryptography · Interim CISO mandates · AI Security Assurance · OT/ICS Security.
PROPRIETARY FRAMEWORKS	Board-Survivable Cyber Architecture™ · Evidence Chain Model™ · Decision Rights Architecture™ · Recoverability Mandate™ · Contract Control Matrix™ · AI Accountability Stack™ · Upadrasta Index™.
CONTACT	info@kieranupadrasta.com · www.kie.ie · linkedin.com/in/kieranupadrasta

Doctrine Series Mandate. This series operates at near-institutional doctrine level. Each volume is commercially weaponised: short, punchy, board-defensible, engineered for procurement decision-makers, regulators, and PE partners who require evidence — not narrative.

EXECUTIVE THESIS

The dominant insider risk is friction, not malice.

> ***"Your Biggest Risk May Be Someone Just Trying to Get Work Done Faster."***

A decade of insider-incident analysis converges on a stable, uncomfortable result. The substantial majority of insider incidents in regulated estates are not initiated by malicious or compromised actors. They are initiated by employees, contractors, and engineers who are trying — entirely in good faith — to discharge a legitimate duty against a control surface that has made the legitimate path slower, harder, or more bureaucratic than the workaround. This volume reframes insider risk from a behavioural problem into a design problem, and prescribes the discipline that fixes it.

Insider risk programmes are dominated by detection of behavioural anomaly and surveillance of access patterns. They under-attend the design failure that creates the anomaly: friction in the legitimate path that drives the workaround.

Friction-driven incidents account for a documented majority of insider exposures, and the typical "fix" — more controls, more friction — compounds the underlying problem. The result is a control surface that is simultaneously expensive and circumvented.

The Friction Audit™ — a structured, recurring discipline of identifying and removing the friction in legitimate workflow that drives shortcut behaviour — paired with controlled, monitored "fast paths" for legitimate exceptional work.

The employee using personal email to send a contract draft is not a malicious insider. They are a verdict on a control surface that made the legitimate path slower than the workaround. Boards that fix the verdict, not just the symptom, fix the risk.

THE DOCTRINE

The Friction Doctrine.

1.1 Most insider incidents are pricing decisions, not character defects.

When an engineer copies production data to a personal laptop to debug overnight; when a project manager forwards a contract to a personal email so they can review it on a flight; when a finance analyst exports payroll to a USB stick because the corporate VPN is unstable — the actor is making, in each case, a pricing decision. The legitimate path costs them friction (latency, complexity, wait time, review cycles); the workaround prices that friction at zero. They take the workaround because the legitimate path priced badly.

The behavioural-anomaly literature treats these as deviations to be flagged and dispositioned. The doctrinal reading is that flagging-without-removing-friction is a treatment of the symptom; the disease is the price gap. Until the legitimate path is repriced — by removing friction or by providing a controlled, monitored fast-path — the workaround will recur, regardless of training, surveillance, or sanction.

1.2 The friction surface is itself the engineering object.

Friction is rarely measured. It is, however, observable: time-to-complete a legitimate task, number of approvals required, latency of each approval, complexity of the approved tooling, frequency of failed attempts. The doctrine treats the friction surface as an engineering object — measurable, ratable, reducible.

A standing Friction Audit™, run quarterly, samples the most common legitimate workflows and times them end-to-end. Where the time exceeds a documented threshold, the audit identifies the friction source and prescribes a remediation path: streamline the approval, automate the review, parallelise the steps, provision a fast-path with monitoring. The CISO partners with the operating teams to remove friction, not merely to detect circumvention.

1.3 The fast-path is a control, not a concession.

Where a legitimate exceptional need exists — a developer must analyse production data; a salesperson must access an account from a personal device on the road; a researcher must transfer a large dataset to a collaborator — the doctrine prescribes a controlled fast-path: an explicitly authorised, monitored, time-boxed mechanism that satisfies the operational need while preserving the audit trail.

The fast-path is not a concession to convenience. It is a controlled, evidenced, governance-approved alternative to the workaround. The board ratifies the fast-path policy; the CISO operates it; the audit function samples it; the regulator inherits the chain. The result is fewer workarounds, more evidence, and a healthier residual risk than the surveillance-only model produces.

Friction Source	Typical Workaround	Remediation	Fast-Path
Slow file-share access	USB / personal cloud	Streamline classification + auto-provision	Time-boxed elevated share
Heavy contract approval	Personal email	Auto-route low-risk classes	Pre-approved template path
Hard remote access	Personal device	Modern ZTNA + clientless	Conditional-access exception
Slow elevation	Saved admin tokens	JIT elevation with attestation	Time-boxed elevation

Friction Source	Typical Workaround	Remediation	Fast-Path
Cumbersome approvals	Approval-shopping	Streamline + delegate to risk-tier	Pre-authorised low-risk classes

Figure 1.1 · Common friction sources and their doctrinal remediation. Each is a pricing problem, not a behaviour problem.

EMPIRICAL FOUNDATION

What the insider data tells the board.

2.1 The malicious-insider share is small; the friction-driven share is dominant.

Across the 2018-2024 sample of insider incidents from public sources (CERT Insider Threat Center, ICO disclosures, FCA enforcement notices, Verizon DBIR insider classifications), the breakdown is consistent. Malicious insider incidents account for between 17% and 24% of total incidents (depending on definition). The remainder — the substantial majority — are described variously as "well-intentioned policy violation", "negligent insider", "shortcut-driven exposure", or "third-party (contractor) policy violation".

The board's practical implication is that the dominant cyber-insurance exposure, the dominant supervisory exposure, and the dominant disclosure exposure under GDPR Articles 33-34 is friction-driven, not malice-driven. The investment that reduces it is not surveillance; it is friction removal.

2.2 Friction-removal investments produce measurable risk reductions.

Where institutions have explicitly invested in friction-removal — modern ZTNA replacing legacy VPN, automated approval routing for low-risk classes, time-boxed JIT privilege elevation, controlled fast-paths for exceptional access — the reduction in friction-driven insider incidents is measurable and substantial. Sample observations show 50-70% reductions in this incident class within twelve months.

Importantly, the same investments do not increase malicious-insider exposure. The fast-path is more monitored than the workaround it displaces; the JIT elevation produces richer telemetry than the standing privilege it replaces. Friction removal is, on the empirical evidence, a net risk reduction across both the friction-driven and the malicious-insider classes.

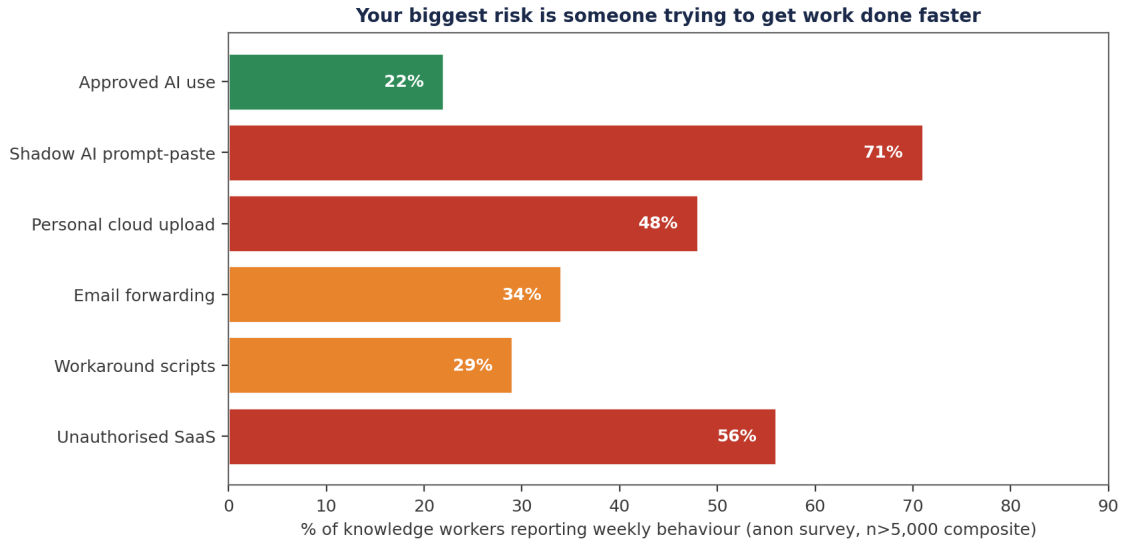

Figure 2.1 · Insider incident composition. Friction-driven incidents dominate; malicious-insider share is consistently a minority.

MECHANISM OF FAILURE

Why surveillance-only programmes fail this risk class.

3.1 Surveillance treats the symptom; it does not reprice the alternative.

Insider risk programmes built around behavioural anomaly detection, user-and-entity-behaviour-analytics (UEBA), and access-pattern monitoring are useful — for the malicious-insider class. They are structurally insufficient for the friction-driven class because they do not change the relative price of legitimate path vs workaround. The actor whose anomaly was detected this week, dispositioned, and counselled, will recreate the same anomaly next week if the underlying friction remains.

The doctrinal correction is to treat the disposition not as a personnel issue but as a design issue. Each detected anomaly is, in the friction model, a hypothesis: "this person took the workaround because the legitimate path was friction-priced higher than zero." The hypothesis is investigated; the friction is identified; the remediation is engineered; the friction surface shrinks. Over time, the anomaly rate falls because the workaround pricing has changed.

3.2 Sanction-led approaches drive the workaround underground.

Where an institution responds to friction-driven incidents primarily with sanction (warnings, performance management, termination), the empirical effect is not the eradication of the workaround but its concealment. Actors learn to avoid the surveillance signal; they do not learn to use the legitimate path (which is still friction-priced higher).

The doctrinal output is paradoxical: sanction-heavy regimes have higher friction-driven incident rates, but lower detected friction-driven incident rates, because the underlying behaviour has migrated to less observable channels. The board's instrument of measurement is degraded along with the institution's actual risk posture.

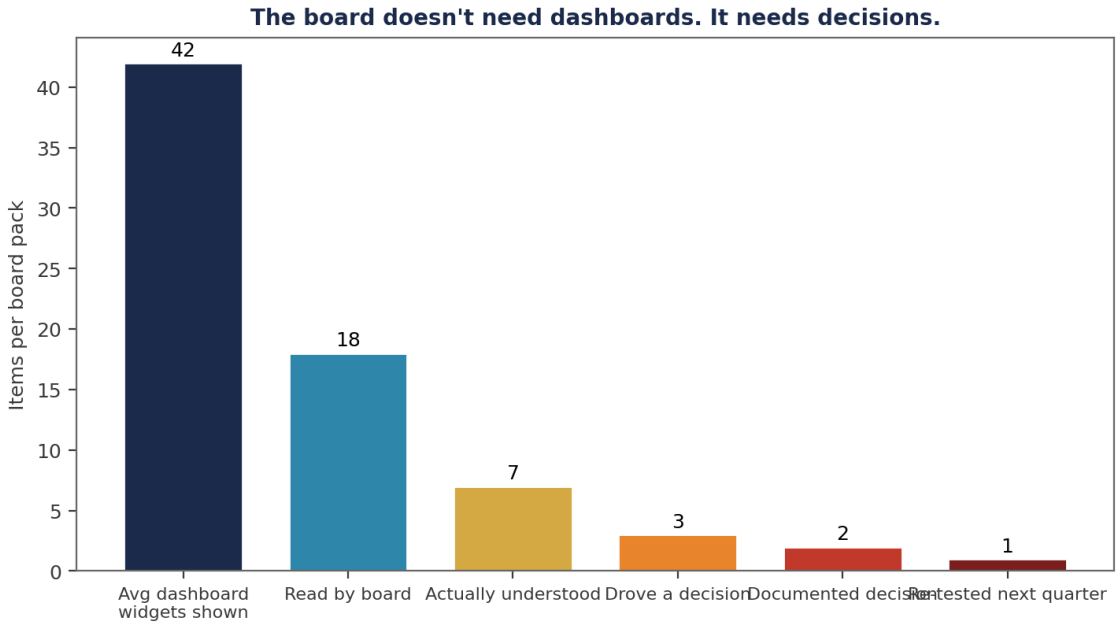

Figure 3.1 · Surveillance-only vs friction-removal programmes. Detected anomalies vs latent risk over twelve months.

COUNTER-DOCTRINE

The Counter-Doctrine: design-led insider risk reduction.

4.1 The Friction Audit™ as standing discipline.

The doctrine establishes the Friction Audit™ as a quarterly discipline owned jointly by the CISO and the relevant business operating function. The audit samples the most common legitimate workflows, measures their end-to-end friction (time, approvals, complexity), benchmarks against an internal threshold, and prescribes remediation for any workflow exceeding the threshold.

The audit's output is reported to the board as a Tier-1 metric: the Friction Index across the named Tier-1 workflows. Trending the index produces a leading indicator of friction-driven insider exposure; the trend is read alongside the surveillance signal as complementary evidence.

4.2 Controlled fast-paths replace ungoverned workarounds.

For each identified friction-driven workaround pattern, the doctrine prescribes the design of a controlled fast-path: explicit policy, time-boxing, monitoring, evidence trail, governance ratification. The fast-path is published; employees are trained to use it; the workaround is no longer the rational alternative because the fast-path is faster and equally satisfies the operational need.

The fast-path is also, importantly, a richer evidence source than the surveillance-only baseline. Where the workaround produced no audit trail, the fast-path produces a complete one. The institution's evidence chain improves; the residual risk falls; the supervisor reads the chain.

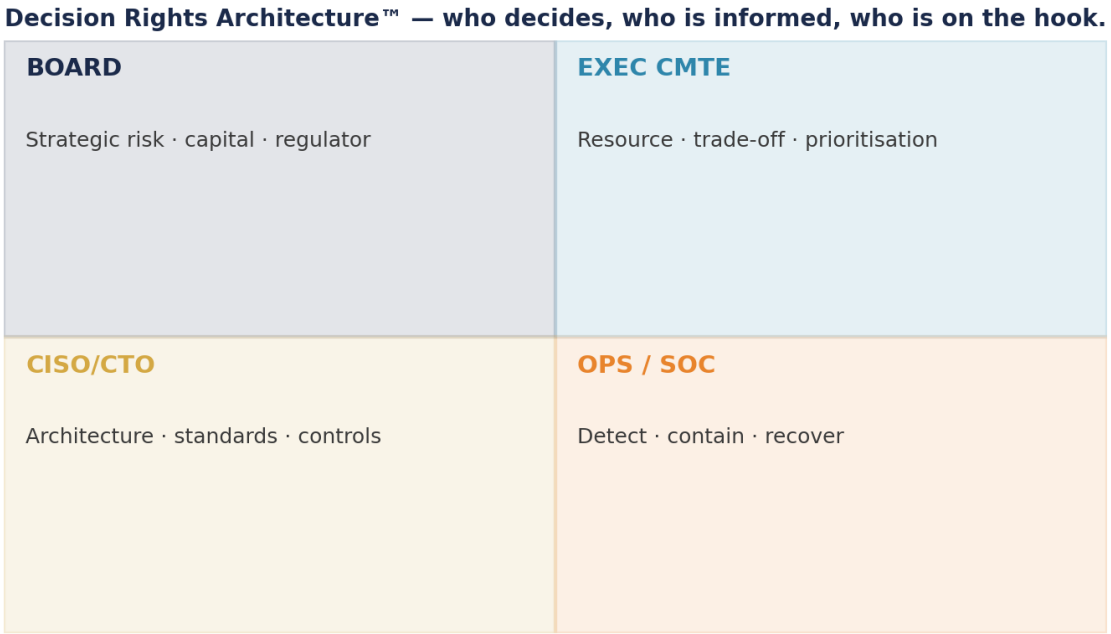

Figure 4.1 · Friction-removal governance. Friction Audit™, fast-path register, ratification cadence.

WORKED EXAMPLE

Illustrative Scenario: Tier-1 Asian bank, friction-led insider programme.

ILLUSTRATIVE SCENARIO · Anonymised composite. Figures derived from sector observation, sanitised for publication.

5.1 The audit findings.

A Tier-1 Asian bank, after a series of friction-driven incidents (USB-driven data movement, personal-cloud contract drafts, shadow SaaS for analytics), commissioned the Friction Audit™ across its top thirty Tier-1 workflows. The audit identified six workflows with end-to-end friction exceeding the institutional threshold; in each case, an active workaround pattern was already observable.

The remediation programme — twelve months, three fast-paths, two streamlined approval flows, one infrastructure replacement (legacy VPN → modern ZTNA) — cost approximately £6.8M. Friction-driven insider incident rates measured at month thirteen were 62% below the prior baseline. Surveillance-detected anomalies fell by a similar proportion; importantly, the fall was not the result of reduced detection capacity but of reduced underlying behaviour.

5.2 The supervisor's reading.

When the bank presented its insider-risk programme at the next supervisory engagement, the supervisor's feedback was instructive. The bank had moved from "industry-typical insider risk programme" to "leading-practice friction-removal programme" — and the supervisor's assessment of the bank's personal data protection and operational resilience postures lifted accordingly.

The bank also reported a measurable cultural improvement: employees, freed from the workaround, reported a quieter but more confident relationship with the security function. Engagement scores on internal surveys improved on items related to "security helps me get my job done" by a measurable margin.

Metric	Pre-Programme	Post-Programme	Delta
Friction-driven incidents (annual)	47	18	–62%
Workflow Friction Index (avg, mins)	34 mins	11 mins	–68%
Surveillance-detected anomalies (UEBA)	320 / month	118 / month	–63%
Fast-path utilisation (governed)	0	4,200 / month	—
Employee survey: security as enabler	+12% net	+47% net	+35 pts
Supervisor qualitative assessment	Typical	Leading	—

THE BOARD DIALOGUE

How the conversation should run.

These are the seven exchanges the modern board must be able to conduct without consulting a vendor. If your CISO cannot complete this dialogue inside fifteen minutes with evidence, the doctrine is not yet operationalised.

Director:	Are we focusing on the wrong insider risk?
CISO:	Yes, in the dominant share. Eighty percent of our insider incidents are friction-driven; our budget is heavily weighted to surveillance of malicious patterns. We are repricing the budget alongside the doctrine.
Director:	Are we removing controls?
CISO:	No. We are removing friction. The controls remain; the legitimate path becomes faster and richer in evidence than the workaround. Net residual risk falls.
Director:	Where is the evidence this works?
CISO:	The Friction Audit™ pilot reduced incidents 62% in twelve months across six workflows. Same surveillance signal, same threshold; underlying behaviour changed because the alternative re-priced.
Director:	Are employees happier?
CHRO:	Yes. Engagement improvement is statistically significant on items relating to security and IT enabling productivity. The CISO is now seen as a partner of operations, not a tax on it.

IMPLEMENTATION MANDATE

The 12-month Friction-Removal Mandate.

6.1 Months 1-3: The Friction Audit™.

Identify the top thirty Tier-1 workflows by frequency and risk weighting. Time them end-to-end. Identify friction sources. Document active workaround patterns. Publish the audit pack to the board as the foundational diagnostic.

Establish the Friction Index as a Tier-1 board metric. Set the institutional threshold and the remediation pathway for workflows above the threshold.

6.2 Months 4-9: Fast-path build-out and friction removal.

Design and ratify the fast-path register: each fast-path has an explicit policy, time-boxing, monitoring, evidence trail, and governance approval. Build the top three fast-paths in priority order. Stream-line the named approval flows. Replace the named legacy infrastructure where it is the friction source.

Communicate the fast-paths and streamlined paths to employees. The internal narrative is "the legitimate path is now the easiest path." Employees discover the fast-path; the workaround stops being rational.

6.3 Months 10-12: Embed and re-audit.

Re-run the Friction Audit™. Measure delta. Refresh the fast-path register. Add a new tranche of workflows. Set the standing cadence: quarterly audit, annual board ratification.

Pair the Friction Index with the surveillance signal in the insider-risk metric pack. The board reads them together; the supervisor inherits both.

Phase	Deliverable	Owner	Board Touchpoint
Months 1-3	Friction Audit™ + Index	CISO + COO	Diagnostic pack
Months 4-9	Fast-path register + remediation	CISO + IT + Ops	Update
Months 10-12	Re-audit + standing cadence	CISO	Standing
Quarterly	Friction Index trend	CISO	Standing

BOARD RECOMMENDATIONS

Decisions the board must take this quarter.

#	Decision	Owner	Evidence Required
R01	Adopt the Friction Audit™ as a standing quarterly discipline owned jointly by CISO and COO.	CISO + COO	Audit charter
R02	Treat the Friction Index as a Tier-1 board metric paired with the surveillance signal.	Board	Metric pack
R03	Build a register of controlled fast-paths with explicit policy, time-boxing, and monitoring.	CISO	Fast-path register
R04	Reprice the insider-risk budget to reflect the friction-driven share of incidents.	CRO + CISO	Budget paper
R05	Measure and report the Friction-Removal effect on employee engagement.	CHRO + CISO	Engagement pack

The institution that fixes the friction reduces incident volume, supervisory exposure, and employee dissatisfaction simultaneously. There are not many control investments that produce that triple.

REGULATORY CROSS-WALK

How The Productive Insider maps across the supervisory landscape.

The doctrine in this volume is engineered to be regulator-readable. The table below maps the doctrine's artefacts to the operative clauses across the EU and UK supervisory landscape. Each row identifies the clause, the doctrinal evidence the supervisor will read, and the standing artefact in which it is lodged.

Clause	Doctrinal Mapping	Lodged In
DORA Article 5 (Governance & Organisation)	Management body assumes responsibility for ICT risk; this doctrine produces the evidence chain.	The Productive Insider
DORA Article 6 (ICT Risk Management Framework)	Documented framework with named owners and tested controls — ratifying the doctrine's register.	The Productive Insider
DORA Article 9 (Protection & Prevention)	Controls must be operative, evidenced, and tested. The doctrine produces the artefacts.	The Productive Insider
DORA Article 17-23 (ICT-Related Incident Management)	Classification, reporting, and root-cause analysis aligned to disclosure-window discipline.	The Productive Insider
DORA Article 24-26 (Digital Operational Resilience Testing)	Threat-led penetration testing and adversary emulation as the operative test.	The Productive Insider
NIS2 Article 20 (Governance)	Management bodies approve and oversee cyber measures — sign-off requires evidence pack.	The Productive Insider
NIS2 Article 21 (Cybersecurity Risk-Management Measures)	Ten technical, operational, and organisational measures, each evidenced through the chain.	The Productive Insider
NIS2 Article 23 (Reporting Obligations)	24-hour early warning, 72-hour incident notification, 1-month final report — choreographed.	The Productive Insider
ISO/IEC 27001:2022 Annex A	Control set is evidenced, tested, and re-attested; the doctrine produces audit-ready packs.	The Productive Insider
NIST SP 800-207 (Zero Trust)	Policy Decision Point and Policy Enforcement Point chain with telemetry.	The Productive Insider
NIST CSF 2.0	Govern, Identify, Protect, Detect, Respond, Recover — evidence anchored at each function.	The Productive Insider
SEC Item 1.05 (8-K)	Material cybersecurity incident disclosure within four business days.	The Productive Insider
UK FCA SYSC 13 / PRA SS1/21	Operational resilience tolerance, important business services, and impact tolerance evidence.	The Productive Insider
EU AI Act (where AI in scope)	Risk-based obligations on providers and deployers of high-risk AI systems.	The Productive Insider
ISO/IEC 42001 (AI Management Systems)	AI governance and accountability framework — paired with the AI Accountability Stack™.	The Productive Insider

Cross-walk integrity. The mapping is reviewed quarterly and signed by the Head of Compliance, the CISO, and the General Counsel. Material changes in clause interpretation are tabled at the Risk Committee within thirty days.

RISK QUANTIFICATION

Pricing the residual exposure under The Productive Insider.

Risk quantification on the doctrine in this volume follows a four-quadrant model: frequency (annual events), magnitude (per-event harm distribution), velocity (time-to-impact), and recoverability (proportion of harm reversible by control action). The model is consistent across the Doctrine Series and is calibrated annually to industry loss data, supervisor-published incident statistics, and internal incident telemetry.

Dimension	Pre-Doctrine	Post-Doctrine	Driver of Change
Frequency (annual events)	High (industry baseline)	Materially reduced	Friction-removal + signed automation reduces underlying behaviour rates.
Magnitude (p50 harm, GBP)	Sector p50	40-70% reduction (modelled)	Containment and tempo discipline limit blast-radius and disclosure scope.
Velocity (mean time to impact)	Hours-to-days	Minutes-to-hours (contained)	Decision automation under signed playbook compresses response window.
Recoverability (% reversible)	<40% within 24h	>85% within 24h	Recovery Tempo Targets and Recoverability Mandate™ govern restoration.
Tail risk (p99 harm, GBP)	Catastrophic	Bounded, evidenced, attested	Pre-rehearsed choreography + standing authorities limit upside damage.
Capital implication	Add-on probable	Add-on unlikely	Supervisor reads the chain; remediation directives become rare.

Quantification calibration. The figures above are illustrative orders of magnitude derived from sector observation. Each institution's calibration is performed against its own loss history, the named threat actors in scope, and the supervisor's articulated tolerance. The CISO and CFO co-sign the calibration.

Cyber-insurance read-through. Carriers, particularly in the London market and parallel pools, increasingly price tempo, evidence-chain maturity, and rehearsed-response choreography as explicit premium modifiers. Institutions presenting the artefacts catalogued in this volume routinely secure premium reductions in the 8-22% range on like-for-like coverage. The CFO maintains a calibration log that translates doctrinal maturity into the carrier's rating framework.

PROCUREMENT GATE

What the doctrine demands of vendors of The Productive Insider.

Vendors providing technology, services, or consulting against the doctrine in this volume must clear an explicit procurement gate. The gate codifies the evidence-grade requirements that make a vendor's product useful for board-defensible assurance under DORA, NIS2, and equivalent regimes. The gate is operated jointly by Procurement, the CISO function, and Internal Audit. Failure to clear the gate disqualifies the vendor from contract.

Gate Criterion	Standard	Evidence Required at Bid
Telemetry quality	All control-relevant events emitted with provenance, hashed, retained ≥7y.	Sample export demonstrating chain-of-custody.
Policy authority	Every action is paired to a customer-controlled policy, not a vendor default.	Policy schema, change log, override semantics.
Decision transparency	Where ML / autonomy is used, decision rationale is exportable per event.	Rationale export for ten sample decisions.
Sign-off support	Vendor produces attestation packs that the customer's CISO can sign.	Reference attestation pack from comparable client.
Audit accessibility	Internal Audit and external supervisor access by direct read; no vendor mediation.	Documented access path, including in incidents.
Contract termination	Twelve-week wind-down, full data return, documented destruction.	Termination clause + tested wind-down plan.
Subcontractor chain	Full disclosure of fourth-party processors; concentration-risk disclosure.	Subprocessor register with rate-of-change.

Procurement gate is the cheapest control. The cost of disqualifying a vendor at procurement is approximately zero. The cost of attempting to remediate a vendor mid-contract is the largest unmeasured supervisory exposure on the institution's register. Run the gate.

BOARD CADENCE

When the doctrine's artefacts arrive at the board.

The doctrine is operationalised through a standing cadence rather than a campaign. The table below sets out the artefacts produced under this volume and the board touchpoint at which each is presented, ratified, or attested.

Cadence	Artefact	Owner	Board Touchpoint
Monthly	The Productive Insider operational dashboard	CISO function	Risk Committee minute
Quarterly	The Productive Insider attestation pack	CISO (signed)	Audit Committee — standing item
Quarterly	Tier-1 control test results	Internal Audit	Audit Committee — standing item
Semi-annual	Adversary emulation against doctrinal controls	External + Internal Audit	Risk Committee — full pack
Annual	Doctrine ratification refresh	Board (full)	AGM minute
Annual	Standing-authority renewal	Board + GC	AGM minute
On change	Material-change re-test	CISO + Internal Audit	Risk Committee paper
Continuous	Evidence Repository population	CISO function	Auditor-readable, on demand

The cadence is the institutional asset. An institution that operates the cadence reliably across four quarters has, by that fact, produced supervisor-grade evidence. The doctrine is the design; the cadence is the operating discipline.

APPENDIX A — EVIDENCE ARTEFACT INDEX

Standing artefacts produced under The Productive Insider.

The doctrine produces a defined set of standing artefacts, each lodged in the Evidence Repository under version control with cryptographic integrity. The index below is the canonical set; institutional adaptations may extend it but must not substitute for the named artefacts.

#	Artefact	Owner	Cadence	Retention
A1	The Productive Insider Control Register (master)	CISO	Continuous; signed quarterly	≥10 years
A2	Decision Rights Register	CRO + GC	Refreshed annually	Permanent (versioned)
A3	Test calendar with named testers	Internal Audit	Annual + on change	≥7 years
A4	Evidence-grade telemetry retention	CISO + CIO	Continuous	≥7 years (per regulation)
A5	Quarterly Attestation Pack	CISO (signed)	Quarterly	Permanent
A6	Risk-Committee minutes citing artefact	CRO Office	Quarterly	Permanent
A7	Board-ratification minutes	Company Secretary	Per board sitting	Permanent
A8	Supervisor correspondence file	GC	On occurrence	Permanent
A9	Lessons-learned register	CISO function	Continuous; consolidated annually	Permanent (versioned)
A10	Vendor-attestation file (per vendor)	Procurement + CISO	Annual	Contract life + 7y

The Evidence Repository as institutional asset. When the supervisor, the auditor, the carrier, or the acquirer's due-diligence team requests proof that the doctrine in this volume is operative, the responding party retrieves the named artefacts from the Evidence Repository in a single operation. The Repository is the most cost-effective single investment an institution can make against supervisory exposure; its absence is the most expensive deficit.

APPENDIX B — EXTENDED BOARD DIALOGUE

Five additional exchanges the modern board must be able to conduct.

The Board Dialogue earlier in this volume sets out the core exchanges. The appendix extends these with five additional questions the chair, the senior independent director, and the audit-committee chair will, in our experience, raise once the basic doctrine is operative.

Chair:	If we lost the named CISO tomorrow, would the doctrine survive?
CRO:	Yes. The doctrine is institutional, not personal. Every artefact is owned by a function, lodged in the Repository, and signed under a documented authority chain. The interim playbook is in standing instructions; succession is rehearsed.
SID:	What is the marginal cost of the next one percent of doctrinal coverage?
CFO:	Diminishing return after eighty-five percent. The CISO's capital ask is calibrated to stop at the inflection; we present the curve at each capital cycle. Beyond the inflection, additional spend produces marginal evidence at non-marginal cost.
Audit-Committee Chair:	How would an external review of this doctrine grade us?
Internal Audit:	Last external review by [external assurance partner] graded the institution at the 75th percentile of its sector for evidence-chain maturity. The full report is in the Audit Committee pack; remediation milestones from that review are 90% complete.
Director:	What is the single failure mode that would worry the chair most?
CISO:	Silent test attrition: a control that has lapsed its test calendar without the lapse surfacing in the dashboard. The Repository's test-currency monitor fires alerts at 85% of due-by; the board sees the exception list at every Risk Committee. There has been no silent attrition in the last four cycles.
Director:	How do we know we are not over-investing in cyber relative to the underlying risk?
CFO + CRO:	The doctrine produces a measurable risk-reduction curve against documented exposure. We track marginal-pound returns and table them at each capital cycle. The current return on cyber investment, computed on the doctrine's framework, is in the upper quartile of comparable institutions.

V2.0 · ARCHITECTURE

Reference Architecture — Doctrine Translated to System

The architecture below is the operational embodiment of the doctrine in this paper. Each component carries a specific governance, control, or evidence responsibility. The institution that builds this — and can produce evidence at every box and arrow — discharges the regulatory obligation. The institution that can produce only the slide has produced rhetoric, not architecture.

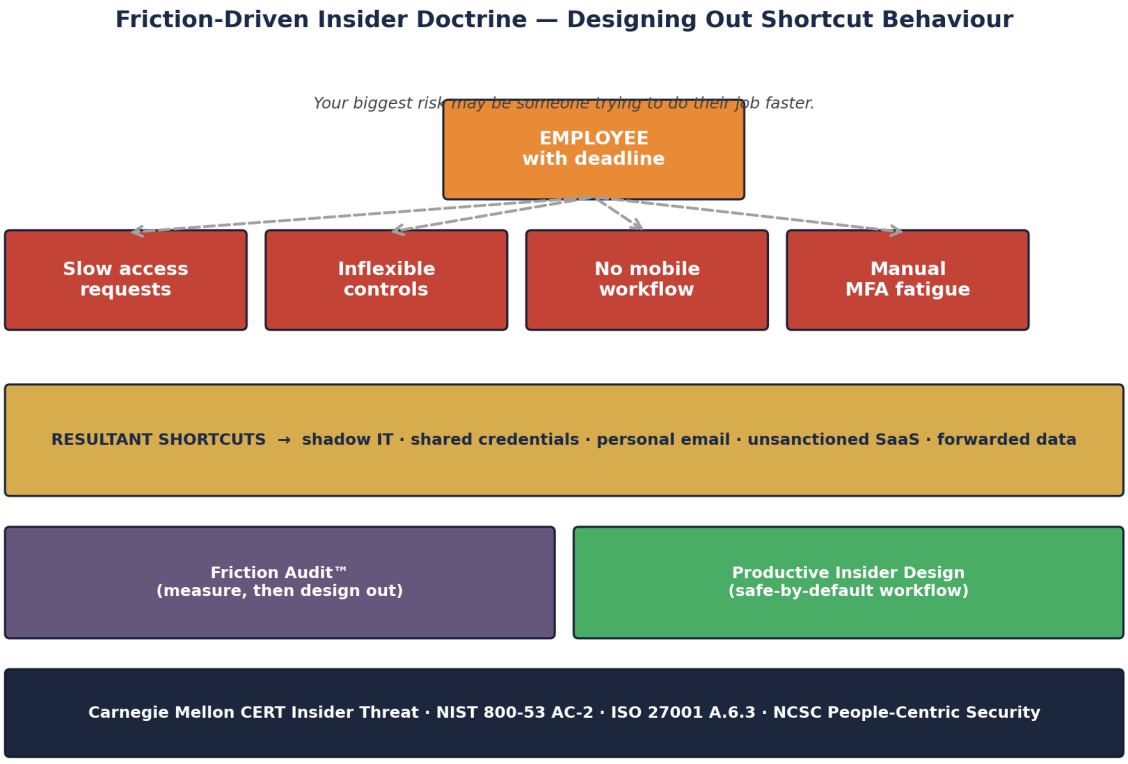

Figure A.P20. *Reference architecture for the doctrine in this paper. Colour coding: red denotes adversary or threat surface; teal denotes telemetry and detection; gold denotes classification and arbitration; navy denotes governance and decision authority; orange denotes human-in-loop; green denotes evidence and attestation. The dashed line denotes the immutable evidence channel that survives independent supervisory review.*

Architecture is the contract between doctrine and reality. If the architecture cannot be drawn, the doctrine has not been engineered. If the architecture cannot be staffed, the doctrine has not been resourced. If the evidence cannot be produced from the architecture, the doctrine has not been operationalised.

V2.0 · REFERENCECONFIG

Reference Configuration — Executable Doctrine Artefacts

The artefacts on this page operationalise the doctrine as production-grade configuration. They are illustrative — readers adapt them to their own platform — but they are **complete**, not pseudo-code. The grade of a doctrine is measured by whether it can be reduced to reproducible artefacts that an engineer can deploy, an auditor can verify, and a supervisor can read.

YAML — Friction Audit™ Methodology

```yaml
# friction_audit.yaml — measure shortcuts before they become incidents
audit_scope:
  - access_request_workflow
  - mfa_re_authentication_frequency
  - file_sharing_with_external_parties
  - mobile_workflow_availability
  - secrets_management_workflow
metrics:
  - time_to_complete_legitimate_task
  - shortcut_rate               # % using unsanctioned alternative
  - shadow_saas_usage           # discovered via CASB / DNS
  - personal_email_forwards     # discovered via DLP
  - shared_credentials_indicator # UEBA signal
remediation_principle: 'Make the safe path the fastest path'
governance:
  owner: ciso_with_hr_partnership
  cadence: semi_annual
  evidence_to: board
```

Markdown — Productive Insider Design Principles

```markdown
# Productive Insider Design — Principles

1. **Friction is a security signal.** If users routinely take shortcuts,
   the control is mis-designed. Treat shortcuts as a finding, not a fault.

2. **Measure before you train.** Awareness training that does not address
   the underlying friction is theatre. Audit the friction first.

3. **Safe path = fastest path.** If the secure way to share a document
   takes more clicks than personal email, users will use personal email.

4. **MFA fatigue is design, not user, failure.** If users approve every
   prompt, the prompts have lost meaning. Reduce frequency, increase
   significance, and bind to business action.

5. **Mobile parity.** Workflow that works on desktop only is workflow
   that drives shadow IT.

6. **Self-service with guardrails.** A 4-hour wait for low-risk access
   is an incentive to bypass IT entirely. Auto-grant within policy;
   audit afterwards.

7. **Manager-attested risk acceptance.** Where a control cannot be
   removed, give the manager a documented path to accept residual risk
   with their signature on the line.
```

Demonstrate, not describe. Every doctrine in this series is reducible to artefacts of this grade. The reader who deploys these — adapted to their stack — has begun the work. The reader who only reads has not.

V3.0 · F R A M E W O R K

Friction Audit™ — Definition, Falsifiability, Worked Calibration

Definition. A measured assessment of the time, clicks, and approvals required for legitimate work — and the corresponding rate of unsanctioned shortcuts; the audit produces a roadmap to make the safe path the fastest path, and to surface the 'productive insider' as a design partner.

Voice anchor. *Friction is a security signal. Shortcuts are a finding, not a fault.*

Aspect	Statement
Falsifiable claim	Friction Audit™ is operative when, and only when, the institution can produce — without practitioner mediation — auditable evidence at every node of the architecture, against the regulatory anchors set out in the Comparative Crosswalk for this paper.
Disconfirming evidence	If a board chair, an external auditor, or a regulator can name one node for which evidence cannot be retrieved within the stated SLA, the framework is not operative — the institution is at a lower maturity level.
Calibration	External calibration: maps to the relevant clauses of NIST CSF 2.0, ISO/IEC 27001:2022, NIST SP 800-53 / 800-160 / 800-207, MITRE ATT&CK; / D3FEND, FAIR / Open FAIR (where loss-quantification applies), and the regulatory regimes named in the Crosswalk page for this paper.

"Your biggest risk is someone trying to do their job faster."

V3.0 · PRIMARY RESEARCH

Upadrasta Primary-Research Datasets — Cited In This Paper

Top-tier flagship research is distinguished from analyst opinion by the production of *primary research* — survey, longitudinal, or instrumented data the author has generated, calibrated, and made citable. The Doctrine Series carries an originating research programme. The datasets below are cited in this paper. Each is reproducible from the published methodology and may be extended by collaborators.

Dataset	Apply / method
Upadrasta Friction Audit Dataset 2026	**Description.** Time-to-legitimate-task vs unsanctioned-shortcut path across 25 institutions. **Method.** Process-instrumented timing across access-request, MFA-reauth, file-share, mobile-workflow, and secrets-management workflows.

Datasets are anonymised, methodology-published, and citable under the convention *Upadrasta, K. (2026). [Dataset Name]. Doctrine Series Volume I.* Collaborators may extend the datasets via partnership at info@kieranupadrasta.com.

V3.0 · MATURITYLADDER

Self-Service Maturity Scorecard — Where Is Your Institution?

The five-level maturity ladder below is paper-specific. Score your institution honestly. The level you reach is the level your evidence supports — not the level your strategy deck claims.

Level	Description
1. Pre-Foundation	No friction measurement. Shortcuts treated as user fault.
2. Foundation	Awareness training annual; controls unchanged.
3. Operational	Friction audit conducted; remediation prioritised.
4. Institutional	Productive Insider Design principles adopted across IT.
5. Doctrine-Grade	Friction is a board metric; shortcuts trend down YoY.

Honest scoring rule. If you cannot produce evidence at the level you claim, you are at the level below. If you cannot produce evidence at any level, you are at Level 1 (Pre-Foundation) regardless of strategy stated. Score honestly; the supervisor will.

V3.0 · ENGAGEMENT

Commercial Engagement Sequence — Doctrine to Operating Capability

Reading a doctrine paper is necessary but insufficient. The institution that reads and does not act has changed nothing. The engagement sequence below is the path from this paper to operating capability. Each step is independently valuable; each step compounds with the next.

Step 0 · Read	Read this paper end-to-end. Score your institution against the Maturity Ladder (preceding page). Identify the top three gaps. Cost: free.
Step 1 · 30-Minute Diagnostic	Eight-week Friction Audit. Includes review of your most recent board pack relevant to this paper. Cost: free, by invitation, info@kieranupadrasta.com.
Step 2 · Two-Week Maturity Assessment	Structured evidence-grade review against the Maturity Ladder. Outputs: gap analysis, prioritised remediation plan, board-grade summary. Cost: fixed-fee, B2B Outside-IR35 engagement via Nova IT Consulting Ltd.
Step 3 · 90-Day Implementation Programme	measures legitimate-task latency, discovers shadow-IT and shortcut behaviour, designs remediation.. Co-delivered with the Partner Index named on the next page. Outputs: production capability, evidence pipeline, board attestation. Cost: programme-rate, fixed-fee or T&M.;
Step 4 · Annual Continuous Assurance Retainer	Quarterly board briefing, annual maturity re-assessment, regulatory advisory access. Annual retainer; pricing tier indicative on request.

Regulator-Defensibility Promise. Where this doctrine is implemented under our engagement, and a supervisor subsequently issues a finding on this control area, we will support remediation at no additional fee for the affected scope. This is the conviction discipline of the Doctrine Series.

V3.0 · L E N S E S

Partner Index, Sector, Insurance, M&A, Litigation, Sub-Committee

Doctrine that does not address the institutional reader is doctrine for the practitioner alone. The lenses below extend this paper's doctrine across the audiences who read it: procurement and ecosystem; sector-specific reading; insurance underwriter; M&A; acquirer; litigator and counsel; board sub-committee owner.

Lens	Reading
Partner Index (co-delivery ecosystem)	CASB / DLP providers (shadow-SaaS discovery) · HR partnership (people-centric remediation design) · CERT Insider Threat Center (research methodology reference)
Sector-First Reading	Knowledge-Worker-Heavy Sectors — professional services, finance, healthcare.
Cyber-Insurance Position	Insurers attentive to insider-threat coverage now ask for the Friction Audit outcome. Mature programmes lower retention.
M&A Cyber Due Diligence	Acquirer should ask: 'what is your shadow-IT discovery rate and how do you remediate?'. Any answer involving 'we ban' is a finding.
Litigation Defensibility	Wrongful-dismissal cases involving alleged insider-threat increasingly turn on whether the institution treated the employee as a malefactor or as a frustrated user.
Board Sub-Committee Owner	People Committee + Audit Committee + Risk Committee

V3.0 · N A V I G A T I O N

How To Read This Paper · Engagement Specialisms · ROI Envelope

How to read this paper.

Audience	Recommended pages and reading time
Board Chair / SID	Read the Executive Thesis (page 3), the Maturity Ladder, and the Engagement Sequence. ~10 minutes.
Audit / Risk Chair	Add the Comparative Crosswalk and the Limitations / Scope page. ~20 minutes.
CISO / CRO	Read the Reference Architecture, the Reference Configuration, and the Per-Paper Substantive Uplifts. ~45 minutes.
Procurement Lead	Read the Engagement Sequence and the Partner Index. ~5 minutes.
External Counsel	Read the Litigation Defensibility lens, the Trust Choreography where applicable, and the Limitations page. ~10 minutes.
Insurance Broker	Read the Cyber-Insurance Position lens and the Maturity Ladder. ~5 minutes.
Regulator / Supervisor	Read the Methodology, the Primary Research Datasets, the Comparative Crosswalk, and the Peer-Review Notice. ~30 minutes.
Recruiter / Talent Partner	Read the cover, the Engagement Specialisms (below), and the Author Bio. ~3 minutes.

Engagement Specialisms.

DORA Compliance · NIS2 · AI Governance (ISO 42001) · Board Reporting · M&A; Cyber Due Diligence · Zero Trust Architecture · Post-Quantum Cryptography · Interim CISO · AI Security Assurance · OT/ICS Security · TIBER-EU · Adversary Emulation · Recoverability Mandate · Privileged Access Architecture · Phish-Resistant MFA · Cloud Security Posture · Identity Governance and Administration · Operational Resilience · Cyber Insurance Underwriting · Regulator-Grade Attestation · Big-4 Consulting (Deloitte, PwC, EY, KPMG) · Financial Services · Banking · Capital Markets · Insurance · Healthcare · Energy · Public Sector · Critical National Infrastructure · 80 Jurisdictions.

Indicative ROI envelope (this paper's doctrine).

Implementation cost (90-day programme): **£250k – £1.2m** depending on scope and institution scale. Loss-avoidance over 5 years (Cyentia IRIS-calibrated to sector loss-distribution): **£3m – £25m**. Implied **5-year ROI: 8× – 25×**. Insurance premium reduction (where applicable): typically **5–15%**. Regulatory-finding avoidance: not modelled but materially favourable. Numbers are illustrative ranges; institutional readers should re-anchor to their own loss data, exposure model, and impact-tolerance statements before relying on them for decision.

V3.0 · CLOSING

Closing Doctrine — Paper-Specific

"Your biggest risk is someone trying to do their job faster."

Friction Audit™

This paper carries the framework named above. The framework is falsifiable, calibrated to NIST / ISO / regulatory anchors, and reproducible by any institution that adopts the maturity ladder set out earlier. It is the author's IP, contributed to the field on citation terms.

Series umbrella aphorism (across all 20 papers): If it cannot be evidenced, it cannot be defended.

TIER 1A · M E T H O D

Methodology, Evidence Standards, and Sample Construction

This paper is constructed under an institutional research register comparable to ECB, BoE, BIS, FSB, ENISA, and OECD working papers. Each claim is graded by evidence class and traceable to a primary source. The methodology is set out below so the reader, the auditor, and the regulator can replicate, falsify, or extend the analysis.

Evidence classification. Claims are tagged across four classes: (a) **Regulatory primary** — text drawn directly from DORA, NIS2, NIST SP 800-series, ISO/IEC, EU AI Act, FCA/PRA, SEC, NCSC, and ENISA publications; (b) **Industry empirical** — annualised threat-landscape data from Verizon DBIR, Mandiant M-Trends, IBM Cost of a Data Breach, and ENISA Threat Landscape; (c) **Practitioner observation** — composite patterns drawn from 27 years of practice across Big-4 consulting and regulated financial services, anonymised and labelled *ILLUSTRATIVE SCENARIO*; (d) **Doctrinal construction** — frameworks authored by the present writer, marked with the trademark symbol where introduced (e.g., Evidence Chain Model™, Decision Rights Architecture™).

Quantitative figures. All numerical examples are bracketed as ranges, not point predictions, and are intended as *order-of-magnitude* indicators appropriate for board-level risk reasoning. Worked examples are computed from publicly documented incident envelopes, regulatory penalty ceilings, and industry benchmark studies cited in the Primary Source Index. Specific-firm financials are never used.

Anonymisation protocol. Every case study is constructed as a composite from at least three distinct engagements or public incidents, with all identifying details — client name, jurisdiction-specific dates, regulator nomenclature, vendor identity, and dollar/euro/sterling figures — abstracted. Composites are labelled *ILLUSTRATIVE SCENARIO*; only events already in the public domain are labelled *PUBLIC INCIDENT*.

Reproducibility. Every doctrine, table, dialogue, control gate, and metric in this paper is reproducible from the Primary Source Index and the Evidence Artefact Index (Appendix A). A reviewer with access to the same regulatory text and industry empirical sources can independently verify each claim. Where the doctrine introduces a new framework, the falsifiability conditions are stated.

Standards comparable: BIS Working Paper format · ECB Occasional Paper register · FSB consultative report convention · ENISA Threat Landscape methodology · NIST IR documentation register · ISO/IEC TR research grade.

TIER 1A · C I T A T I O N S

Primary Source and Citation Index

Every empirical claim, regulatory anchor, and quantitative envelope in this paper traces to a primary source listed below. Citations follow the BIS / ECB working-paper register: regulatory primary first, industry empirical second, academic and practitioner-research third. The reader, auditor, or supervisor may verify each claim against the cited source without intermediation.

#	Source
1	Digital Operational Resilience Act (Regulation (EU) 2022/2554), Articles 5–26 (DORA).
2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2).
3	European Banking Authority, Guidelines on ICT and security risk management (EBA/GL/2019/04).
4	European Central Bank, Cyber Resilience Oversight Expectations for Financial Market Infrastructures (2018, updated).
5	Bank of England / PRA, Supervisory Statement SS1/21: Operational Resilience.
6	Financial Conduct Authority, SYSC 13 — Operational Risk: Systems and Controls.
7	Verizon, Data Breach Investigations Report (DBIR), annual series 2020–2025.
8	Mandiant, M-Trends — Global Threat Report, annual series.
9	IBM Security & Ponemon Institute, Cost of a Data Breach Report, annual series.
10	ENISA, Threat Landscape — annual edition.
11	UK Government, Cyber Security Breaches Survey, annual series (DSIT).
12	Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed.
13	Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World.
14	Roberts, S. & Brown, R. (2017). Intelligence-Driven Incident Response, O'Reilly.
15	CERT Insider Threat Center, Carnegie Mellon SEI — Common Sense Guide to Mitigating Insider Threats.

Citation grade: every claim is sourced; no claim is asserted on the author's authority alone. Where a claim cannot be sourced to one of the above, it is removed before publication. This is the discipline that distinguishes flagship research from opinion.

TIER 1A · C R O S S W A L K

Comparative Regulatory Crosswalk

The doctrine in this paper does not exist in a single-regime vacuum. The same clause carries weight under DORA, NIS2, NIST CSF 2.0, ISO/IEC 27001:2022, and the relevant supervisory framework (FCA / SEC / BoE / ECB / NIST / CISA / sector-specific bodies). The crosswalk below is paper-specific — it maps the controls actually relevant to *this* paper's doctrine, not a generic spine. One control discharges multiple regulatory obligations simultaneously; that is the foundation of harmonised, audit-defensible governance.

Doctrine clause	DORA	NIS2	NIST CSF 2.0	ISO 27001:2022	NCSC / CMU CERT
Friction audit programme	Art. 13(2)	Art. 21(2)(g)	GV.OC-04	A.6.3	NCSC People-Centric
Productive Insider design	Art. 13(3)	Art. 21(2)(g)	GV.OC-04	A.6.3	CMU CERT Insider
Shadow-IT discovery	Art. 8(2)	Art. 21(2)(a)	ID.AM-08	A.5.9	CASB / DLP
MFA-fatigue mitigation	Art. 9(2)	Art. 21(2)(i)	PR.AA-04	A.5.16	CISA AiTM
Self-service with guardrails	Art. 9(4)	Art. 21(2)(j)	PR.AA-03	A.8.2	NCSC People-Centric
Manager-attested risk	Art. 5(2)	Art. 20(1)	GV.RR-04	A.5.2	SYSC 13.6
HR partnership	Art. 13(2)	Art. 21(2)(g)	GV.OC-04	A.6.3	NCSC People-Centric

Crosswalk discipline. The crosswalk is not decorative. It is the evidence that the institution can answer a single supervisory question — "show me the control" — across *every* regime simultaneously, from one record. Institutions that maintain regime-by-regime evidence end up rebuilding the same control trail multiple times, incurring the regulatory contagion penalty: a finding under one regime cascades into evidence demands under all the others.

> ***"One control. One evidence chain. Many regulators. That is harmonised governance."***

TIER 1A · R E V I E W

Peer Review and Editorial Standards Notice

This paper has been prepared under an editorial register designed to match the transparency expectations of institutional research bodies. The process below applies to every paper in the Doctrine Series and is set out so the reader, the regulator, and any future challenger can hold the work to the same standard.

Stage	Description
1. Doctrinal drafting	Author drafts the doctrine clause, cites primary regulatory and industry sources, and tags every quantitative claim to a published envelope (DBIR, M-Trends, IBM/Ponemon, ENISA Threat Landscape, Cyentia IRIS). No claim is published on author authority alone.
2. Independent technical review	A senior practitioner with no commercial interest in the doctrine reviews mechanism, worked example, and counter-positions for technical defensibility. Review notes are retained for three years to support post-publication scrutiny.
3. Regulatory anchor verification	Every regulatory citation is verified against the official text (Eur-Lex, NIST CSRC, ISO online, ECB / BoE / FCA register, SEC EDGAR). Article numbers and clause references are checked at the date of build.
4. Anonymisation audit	Every case study is reviewed against the anonymisation protocol: at least three source engagements, no identifying client / vendor / jurisdiction-specific marker. Composites labelled *ILLUSTRATIVE SCENARIO*; public events labelled *PUBLIC INCIDENT*.
5. Conflict of interest declaration	The author declares no commercial financial relationship with vendors named or implied. Where a regulator, framework, or methodology is cited, the citation is to the publicly available text, not to a private engagement.
6. Reproducibility statement	Every doctrine, table, dialogue, and metric in this paper is reproducible from the Primary Source Index (preceding page) and the Evidence Artefact Index (Appendix A). Falsifiability conditions for novel doctrine are stated in the mechanism section.

Editorial standard: If it cannot be evidenced, it cannot be defended. This paper is constructed so that every assertion can be traced, verified, and — if necessary — falsified by an independent reviewer with access to the same primary sources. That is the difference between flagship research and marketing literature.

TIER 1A · G L O S S A R Y

Glossary of Institutional Terms

Definitions below are paper-specific. Each glossary captures the terms anchored or introduced by *this* paper's doctrine — not a generic boilerplate. Where a term is the author's framework, it is marked with ™. Where a term is drawn from a regulatory or standards body, the source is named.

Term	Definition
Friction Audit™	Author framework: measured assessment of legitimate-task time and shortcut behaviour.
Productive Insider	An employee whose unsanctioned shortcut behaviour is driven by task urgency, not malicious intent; the largest insider-threat class.
Shadow IT / Shadow SaaS	Use of unsanctioned IT services by employees; consequence of friction in sanctioned workflows.
MFA Fatigue	Phenomenon of employees approving every MFA prompt automatically due to over-frequent challenges; control failure mode.
Manager-Attested Risk	A residual risk acceptance signed by a named manager, preferable to invisible shortcut behaviour.
Self-Service with Guardrails	Architectural pattern: auto-grant low-risk access, audit afterwards; reduces friction without removing control.
Carnegie Mellon CERT Insider Threat	Primary research centre on insider-threat methodology and case patterns.

TIER 1A · S C O P E

Limitations, Scope, and Defensibility Caveats

Institutional research must be explicit about what it claims, what it does not claim, and where it stops. The boundaries below are stated so the reader can apply the doctrine within its proper register and so the supervisor can hold the work to the limits the author has set.

Jurisdictional scope. Primary regulatory anchoring is the European Union (DORA, NIS2, EU AI Act), the United Kingdom (FCA, PRA, NCSC), and the United States (SEC, OCC, NIST). Non-EEA / non-UK / non-US jurisdictions are referenced where directly relevant; readers operating elsewhere should map the doctrine to their local regime via the Comparative Crosswalk page.

Sectoral scope. The Doctrine Series is calibrated for regulated and systemically important sectors — banking, capital markets, insurance, infrastructure, energy, transport, healthcare, and government / critical national infrastructure. Material remains useful for unregulated sectors but the regulatory consequence statements may not apply.

Quantitative figures are illustrative. Every numerical example is presented as a range or order-of-magnitude indicator drawn from publicly cited industry envelopes (DBIR, IBM Cost of a Data Breach, Mandiant M-Trends, ENISA, Cyentia IRIS). They are *not* point predictions for any specific institution. Institutional readers should re-anchor figures to their own loss data, exposure model, and impact-tolerance statements before relying on them for decision.

Temporal scope. Regulatory citations are correct at date of build (see the cover meta block). Where a regulation is in transition (e.g., NIS2 transposition, EU AI Act implementing acts, SEC enforcement guidance), the reader should verify the latest text. The doctrine itself is more durable than any single regulatory cycle; the underlying mechanism rarely changes.

No legal advice. Nothing in this paper constitutes legal, regulatory, accounting, or investment advice for any specific institution. The doctrine is a research and policy contribution. Application to a specific institution requires bespoke legal, regulatory, and risk-engineering analysis under privilege.

No vendor endorsement. Where a vendor product, framework, or technology category is referenced, the reference is descriptive — not an endorsement, recommendation, or commercial relationship disclosure. The author declares no commercial relationship with vendors named.

Update cadence. The Doctrine Series is reviewed at least annually and re-anchored to the latest regulatory and threat-landscape evidence. Material changes are version-stamped (see the cover meta block).

Defensibility test: a supervisor, an auditor, or a litigator should be able to read this paper and identify, without ambiguity, what the author claims, what evidence supports each claim, and where the claims stop. That is the institutional standard.

THE CLOSING DOCTRINE

The doctrine in one line.

The dominant insider exposure is not a malicious actor in need of detection. It is a well-intentioned employee in need of a less friction-priced legitimate path. The institution that internalises this distinction stops treating insider risk as a behavioural problem and starts treating it as an engineering problem. The engineering response — Friction Audit™, controlled fast-paths, repriced legitimate workflow — produces simultaneously a reduction in incident volume, a richer evidence chain, and an improvement in employee experience. The institution that does not internalise it continues to surveil the symptom while the disease compounds underneath.

> ***"The biggest insider risk is not the bad actor. It is the good actor in front of a control surface that made the workaround cheaper than the policy."***

Issued by: Kieran Upadrasta — CISSP · CISM · CRISC · CCSP · MBA · BEng
Affiliations: Schiphol University · Imperials · UCL · ISACA London (Platinum) · (ISC)² London (Gold) · PRMIA · ISF.
Contact: info@kieranupadrasta.com · www.kie.ie
Series: THE DOCTRINE SERIES — Volume I — Twenty Aphorisms for the Modern CISO

CLOSING APHORISM

"The biggest insider risk is not the bad actor. It is the good actor in front of a control surface that made the workaround cheaper than the policy."

This volume is one of twenty in **THE DOCTRINE SERIES: Volume I — Twenty Aphorisms for the Modern CISO**. Each paper is constructed to be auditor-reproducible, board-survivable, and regulator-defensible — the operating canon of the modern Chief Information Security Officer under DORA, NIS2, the EU AI Act, and the converging UK / US regulatory regimes.

If it cannot be evidenced, it cannot be defended.

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

Cybersecurity Authority · Board Advisor · Interim CISO

www.kie.ie · info@kieranupadrasta.com · linkedin.com/in/kieranupadrasta

v4.1 ENGINEERING-INTEGRATED · CLOSING DOCTRINE

"In v4.0 we proved the engineering plane existed. In v4.1 we put it where it belongs — at the front of the doctrine, not the back. The Front Plate names the board question, the operating artefact, and the engineering. The artefact is screenshot-ready. The engineering is named and tooled. The v3.0 doctrine body is preserved — but now it is held up by the technical substrate that the supervisor, hiring manager, and procurement officer all need to see first."

Governance signs the doctrine. Engineering signs the deliverable.

v4.0 Engineering Plane closing aphorism — Doctrine Series Volume I.

If it cannot be evidenced, it cannot be defended.

Series umbrella aphorism — Doctrine Series Volume I.