WHITEPAPER | TIER 1A — INSTITUTIONAL DOCTRINE EDITION | v5.2

CSAIC Industrial & OT Cyber Doctrine Series · Paper 14 of 20

The Factory You Didn't Know You Bought

Hidden OT Cyber Liability in Industrial Mergers and Acquisitions

"You did not acquire a factory. You acquired its unknown failure modes."

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng · Lead Auditor (ISF)

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

21 Years Financial Services · AI Cyber Security Programme Lead

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

Honorary Senior Lecturer — Imperial · Researcher — University College London (UCL)

Principal Doctrine Author — Cyber Security AI Consulting (CSAIC)

Audience: PE Funds | Infrastructure Funds | Industrial Acquirers | M&A; Advisers | Insurers | Boards

Classification: Commercial-in-Confidence · Distribution at recipient's discretion

www.kie.ie · info@kieranupadrasta.com · University of Schiphol (UOS)

Keywords: M&A; Cyber Due Diligence | Private Equity | Infrastructure | NIS2 | DORA | Integration | ISO 42001

Notice, Doctrine Statement & Tier Conformance

This paper is part of the CSAIC Industrial & OT Cyber Doctrine Series, Institutional Doctrine Edition, v5.2 — Tier 1A Flagship Thought Leadership. v5.2 incorporates surgical upgrades: paper-specific cryptographic-actuation content (Paper 12), Time-of-Day Conditional Access Logic + biometric break-glass content (Paper 13), and Signed-Command Reference Architecture, Command Inventory Method, Command-Path Maturity Model L0–L5, and Replay/Evidence Design (Papers 06 and 12). University affiliation displayed as University of Schiphol (UOS).

Reading Map

- **Boards:** Executive Synthesis, §5, §10, §14, §19, Board One-Pager (Annex D).
- **Operators / Architects:** §3, §4, §6, §11, §23, and the new §28–§31 artefacts.
- **Investors / insurers:** §1, §5, §6, §12, §13, §19.
- **Regulators:** §2, §6, §7, §8, §16, §22, §26.
- **Sceptics:** §26 (Evidence Basis) and §27 (Counterargument & Rebuttal).

Executive Synthesis

M&A; diligence routinely misses the OT cyber estate. The acquirer inherits unmanaged assets, undocumented vendor pathways, fragile controls, and uninsurable exposures that turn day-one synergy assumptions into year-one losses.

“You did not acquire a factory. You acquired its unknown failure modes.”

Three Claims

1. The risk category is now structural.
2. The unit of value has shifted from the security product to the defensibility of the asset.
3. Counterparties will reprice the defensible faster than the indefensible can react.

1. The Inflection — From Cost Centre to Capital Logic

Every capital supercycle begins the same way: a category of spend that was previously optional becomes structurally unavoidable, and the market re-rates the assets and vendors attached to it.

1.1 The Old Model and Why It Failed

Defence was decoupled from the asset. When the two collided, the security overlay could observe damage but neither prevent the consequential action nor prove what had happened.

1.2 The New Model

Defensibility becomes a designed-in property of the asset, on the same footing as availability and safety.

> *“The board will fund what it can price.”*

2. The Six Doctrines

2.1 OT Diligence Is Asset Diligence

Cyber diligence on OT estates is not a sub-discipline. It is asset valuation.

“Cyber diligence is asset valuation.”

2.2 Vendor Pathways Are Inherited Liabilities

Every OEM, contractor, and remote pathway is an inherited liability. Inventory before close.

“What you do not inventory, you inherit.”

2.3 Insurance Reads Diligence

Insurers reprice acquirers based on diligence quality. Bad diligence raises premium for the acquirer's whole book.

“Bad diligence repays the broker, not the buyer.”

2.4 Carve-Out Risks Are Hidden Risks

Carve-outs leave behind cyber dependencies on the parent. Diligence them explicitly.

“Carve-outs hide dependencies.”

2.5 Day-One Posture Is Day-One Decision

Day-one posture is a decision the acquirer must make pre-close, not an assumption.

“Decide the posture before signing.”

2.6 Integration Plans Include Identity

The first 100 days of integration include identity, authority, and access reform.

“Integration is identity work.”

3. Paper-Specific Adversary Economics

Tailored to this paper's threat model.

3.1 Adversary Classes

- Adversaries exploiting integration windows when controls are weakest.
- Insider risk during separation between announcement and close.
- Vendor compromise inherited through M&A; without notice.
- Latent exposures discovered too late to renegotiate price.

3.2 Adversary Economics

Adversary economics favour the 6-month window from announcement to integration. Doctrine moves OT cyber diligence into pre-close, exposing latent liabilities while price renegotiation is still possible.

3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Information Asymmetry	Seller knows the estate; buyer guesses.	Pre-close OT diligence overhaul
Speed Asymmetry	Integration outruns risk discovery.	Day-one posture decision pre-close
Insurance Asymmetry	Bad diligence raises premium across acquirer's book.	Insurer-aligned diligence artefacts

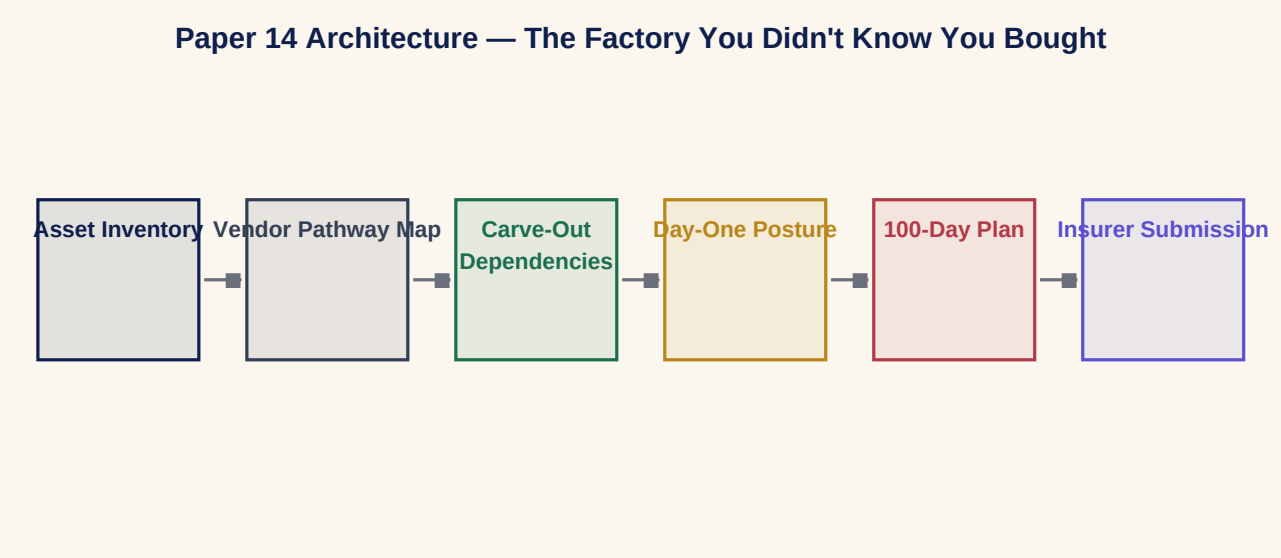
4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

4.1 Four Operating Layers

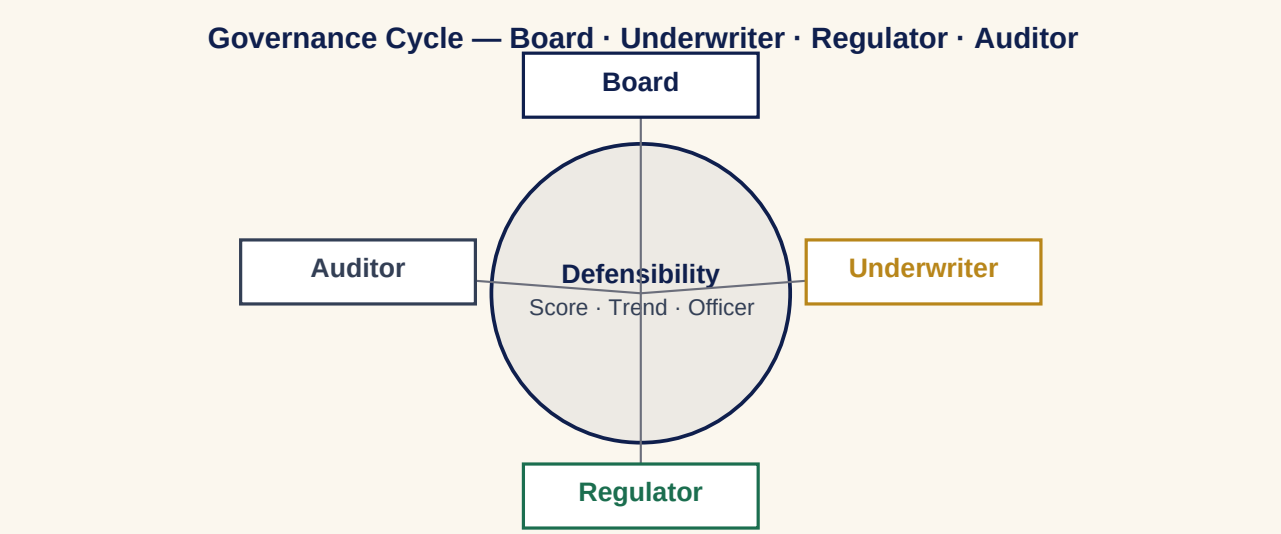
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

4.2 Paper-Specific Architecture Diagram



5. Board Operating Doctrine

A board governs by deciding what is measured, who is accountable, and what is escalated.

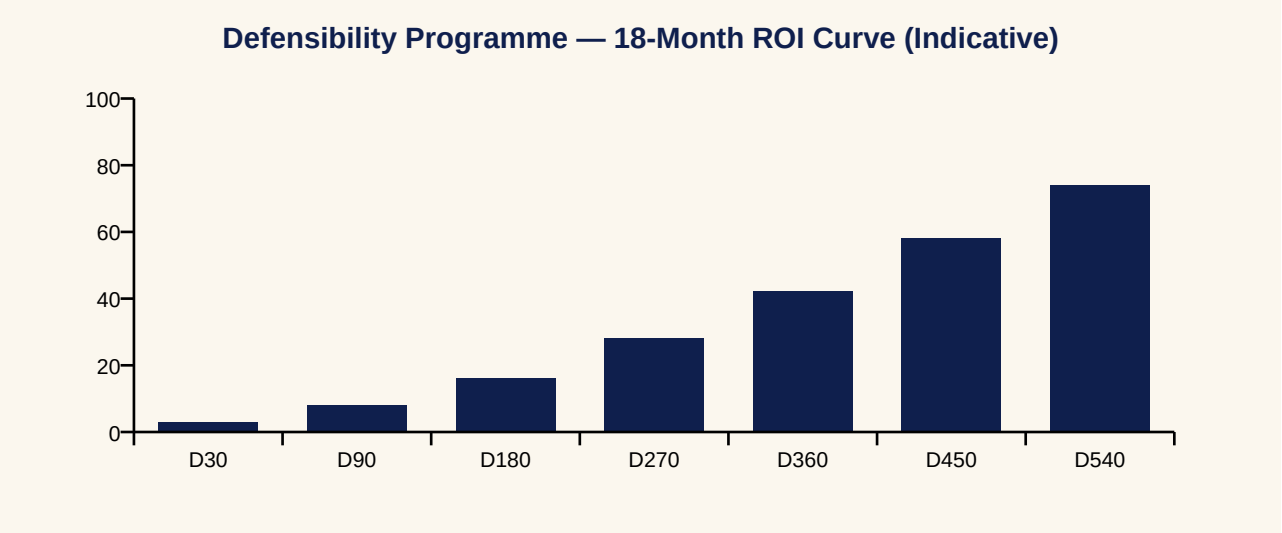


5.1 Three Board Questions

1. What is our defensibility, as a number, and is it improving?
2. Who is accountable for that number this quarter?
3. What would a counterparty say if asked today?

6. Underwriter & Capital-Market Operating Doctrine

Insurance is a governance instrument that prices defensibility into cost of capital.



6.1 Underwriter's Three Questions

1. Can you evidence your posture in time for a real renewal?
2. Can you contain a compromise inside an envelope I can price?
3. Can you produce post-event evidence that lets me pay quickly?

“The board will fund what the insurer can price.”

7. Regulatory & Standards Map — 80 Jurisdictions

Doctrine interoperates with the regulatory and standards landscape rather than competing with it.

#	Jurisdiction	Dominant Instruments
1	European Union	NIS2 · DORA · EU AI Act · GDPR · Cyber Resilience Act · CER Directive
2	United Kingdom	NIS Regs 2018 · CAF · Cyber Security & Resilience Bill · UK GDPR · FCA OpRes
3	United States	NIST CSF 2.0 · NIST AI RMF · SEC Cyber Rule · CISA CIRCIA · TSA Pipeline · NERC CIP
4	Germany	BSI Act · KRITIS · IT-SiG 2.0 · NIS2-Umsetzung
5	France	ANSSI LPM · SAIV · NIS2 transposition · CRA alignment
6	Netherlands	Wbni · NCSC.NL · BIO 2.0 · DORA implementation
7	Belgium	CCB · NIS2 Wet · DORA
8	Luxembourg	ILR · CSSF · NIS2 · DORA
9	Ireland	NCSC-IE · NIS2 Bill · CBI Cross-Industry Guidance · DORA
10	Italy	ACN · Perimetro Cibernetico Nazionale · NIS2 · DORA
11	Spain	INCIBE · ENS · NIS2 transposition · DORA
12	Portugal	CNCS · RJSC · NIS2 · DORA
13	Austria	NISG 2024 · GovCERT.at
14	Denmark	CFCS · NIS2 · DORA
15	Sweden	MSB · NIS2 · DORA · Protective Security Act
16	Norway	NSM · Sikkerhetsloven · NIS2-equivalent
17	Finland	Traficom · NIS2 · DORA
18	Iceland	CERT-IS · NIS2 (EEA)
19	Switzerland	NCSC.ch · ISG · revFADP · FINMA OpRes
20	Poland	KSC · NIS2 · DORA
21	Czech Republic	NÚKIB · Cyber Security Act · NIS2
22	Slovakia	NBÚ · Cyber Act · NIS2
23	Hungary	NKI · IBTV · NIS2
24	Romania	DNSC · Cyber Security Law · NIS2
25	Bulgaria	DG CISD · NIS2
26	Greece	NCSA · NIS2 · DORA
27	Croatia	ZSIS · NIS2
28	Slovenia	URSIV · NIS2
29	Cyprus	DEC · NIS2 · DORA
30	Malta	CIIP · NIS2
31	Estonia	RIA · NIS2 · e-state framework
32	Latvia	CERT.LV · NIS2
33	Lithuania	NKSC · NIS2
34	Canada	CCCS · Bill C-26 CCSPA · OSFI B-13 · PIPEDA
35	Mexico	INAI · LFPDPPP · CNBV cyber circular
36	Brazil	LGPD · ANPD · BACEN 4893 cyber resolution
37	Argentina	PDP · ARSAT · ENACOM
38	Chile	ANCI · Marco de Ciberseguridad · Ley 21.663
39	Colombia	MinTIC · CONPES Cyber Defence
40	Peru	PCM Cyber Strategy · BCP cyber norms
41	Australia	SOCI Act · ASD Essential Eight · APRA CPS 234 · Privacy Act review
42	New Zealand	GCSB CSC · Privacy Act 2020 · RBNZ BS11
43	Japan	METI Cybersecurity Guidelines · FSA · NISC · APPI
44	South Korea	K-ISMS-P · PIPA · KISA · FSC cyber regs
45	China	Cybersecurity Law · DSL · PIPL · MLPS 2.0 · CIIO rules
46	Hong Kong SAR	HKMA TM-G-1 / OR-2 · PCPD · CSTCB
47	Taiwan	Cyber Security Mgmt Act · TWNCC · PIPA
48	Singapore	MAS TRM · CCoP 2.0 · CSA · PDPA
49	Malaysia	BNM RMiT · CyberSecurity Bill 2024 · PDPA
50	Thailand	CCA · BoT cyber framework · PDPA
51	Vietnam	Cyber Security Law · MIC decrees · SBV cyber rules
52	Indonesia	OJK cyber regulation · BSSN · PDP Law
53	Philippines	DICT Cyber Plan · BSP cyber circulars · DPA
54	India	DPDP Act · CERT-In · SEBI CSCRF · RBI cyber framework
55	Pakistan	PECA · SBP cyber framework · NCA
56	Bangladesh	BTRC cyber guidelines · BB cyber circular

#	Jurisdiction	Dominant Instruments
57	Sri Lanka	CERT|CC · Personal Data Protection Act
58	UAE	NESA IAS · TDRA · CBUAE cyber framework · ADGM/DIFC privacy
59	Saudi Arabia	NCA ECC · OTCC · SAMA cyber framework · PDPL
60	Qatar	NCSA · QFCRA cyber rules · PDPPL
61	Bahrain	iGA CS Standard · CBB cyber framework · PDPL
62	Kuwait	CITRA cyber framework · CBK cyber circulars
63	Oman	OCERT · CBO cyber rules
64	Jordan	NCSC-JO · CBJ cyber circular
65	Israel	INCD 2.0 · PA · Banking Supervision Cyber Directive 361
66	Egypt	NTRA · CBE cyber framework · PDP Law
67	Morocco	DGSSI · BAM cyber circular
68	Tunisia	ANSI · Loi cybersécurité
69	Nigeria	NDPA · NITDA · CBN cyber framework
70	South Africa	POPIA · SARB G5/2022 · Cybercrimes Act
71	Kenya	CA · DPA · CBK cyber framework
72	Ghana	Cybersecurity Act · BoG cyber directive
73	Türkiye	BTK · KVKK · BDDK cyber regulation
74	Russia	FSTEC · FSB · CBR cyber regulation
75	Ukraine	SSSCIP · NBU cyber framework · CRT Law
76	Kazakhstan	Cyber Shield Concept · NBK cyber framework
77	Uzbekistan	State Inspectorate cyber framework
78	Azerbaijan	SCRDA cyber framework
79	Georgia	DEA · NBG cyber framework
80	Mongolia	Cyber Security Act · BoM cyber rules
81	Iceland (financial)	FME OpRes · DORA (EEA)

8. Field Dialogues

Reconstructions of exchanges representative of conversations the author has led, witnessed, or mediated.

Setting — Acquirer

Acquirer: We assumed standard hygiene.

Adviser: They did not.

Setting — Insurer

Insurer: Was OT cyber in diligence?

Broker: Yes. Premium adjusted accordingly.

Setting — Board

Director: What did we just buy?

CISO: 12 plants, 47 OEM pathways, and a programme that needs 18m EUR over 18 months.

Setting — Seller

Seller: This is over-diligence.

Acquirer: It is the price of the deal.

9. Case Study — Anonymised Engagement

Anonymised Case Study — Industrial Rollup

9.1 Context

An industrial rollup acquiring three mid-cap targets simultaneously with thin cyber diligence.

9.2 Intervention

Pre-close OT diligence overhaul: asset inventory, vendor pathway inventory, insurer dialogue, day-one posture decision, 100-day plan.

9.3 Outcome

Two targets repriced; one walked away; acquirer's blended insurance premium fell 17%; integration cost reduced through pre-close planning.

10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	OT diligence coverage per target (target = 100%).	Quarterly	CISO / Plant
M2	Vendor pathway inventory completeness pre-close (target = 100%).	Quarterly	CISO / Plant
M3	Day-one posture decisions documented (target = 100%).	Quarterly	CISO / Plant
M4	Insurer-aligned diligence artefacts (target = 100%).	Quarterly	CISO / Plant
M5	100-day plan execution rate (target ≥ 90%).	Quarterly	CISO / Plant

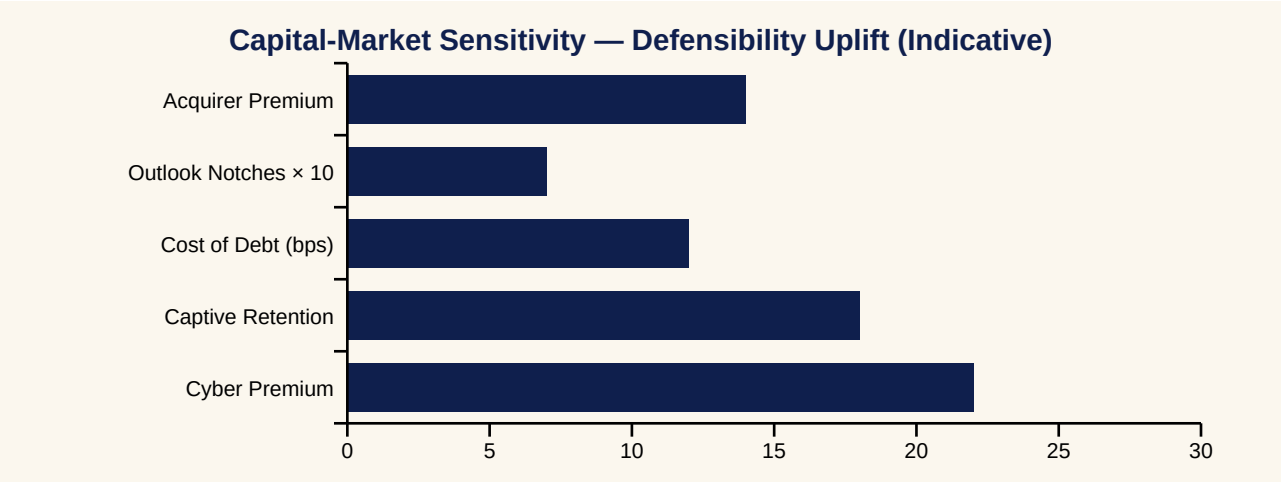
11. Implementation Roadmap — Day 1 to Day 540

Window	Programme Activity	Maturity Stage
Day 1–30	Doctrine adoption. Board commits. Single accountable officer named.	Foundational
Day 31–90	Operating model launched. First insurer dialogue.	Stand-up
Day 91–180	Evidence pipelines live. First quarterly attestation.	Stabilisation
Day 181–360	Continuous cadences operating. Insurer renewal won.	Maturation
Day 361–540	Defensibility published externally. Cost-of-capital benefit captured.	Institutionalisation

12. Press Wire — Quotable Headlines

Outlet Voice	Quotable Headline
Benzinga	PE Funds Discover The 'Factory They Didn't Know They Bought' — A Cyber Diligence Wake-Up
Yahoo Finance	OT Diligence Is Asset Diligence — A Doctrine For Industrial M&A
CNBC	Acquirers' Blended Cyber Premium Falls 17% After Pre-Close Diligence Overhaul
MarketWatch	Day-One Posture Becomes A Pre-Close Decision, Not A Post-Close Assumption
Reuters	Insurers Reprice Acquirers Based On Diligence Quality — Bad Diligence Hits The Whole Book
Financial Times	What You Don't Inventory, You Inherit: A New M&A Cyber Doctrine
Wall Street Journal	100-Day Integration Plans Now Include Identity, Authority And Access Reform
Bloomberg	Carve-Out Cyber Dependencies Become A Standard Diligence Workstream
Barron's	Industrial Rollups Adopt Cyber Diligence As An Asset Valuation Discipline
The Economist	Decide The Posture Before Signing — The New M&A Cyber Doctrine

13. Investor Brief & Valuation Read



13.1 Bloomberg-Style One-Liner

BUY/HOLD signal-improving: The Factory You Didn't Know You Bought doctrine programme reduces operational tail risk.

14. Closing Doctrine — Twelve Lines a Board Should Memorise

"You did not acquire a factory. You acquired its unknown failure modes."

"Cyber diligence is asset valuation."

"What you do not inventory, you inherit."

"Bad diligence repays the broker, not the buyer."

"Carve-outs hide dependencies."

"Decide the posture before signing."

"Integration is identity work."

"Evidence beats effort. Activity is not outcome."

"Counterparties price defensibility before the board does."

"Doctrine outlasts product cycles, frameworks, and threat actors."

"Continuous cadences beat episodic compliance."

"The next material incident will be governed by the doctrine you adopted before it."

15. Methodology & Provenance Statement

- Doctrine derived from more than two decades of practitioner engagement across Big-Four consulting, financial services, energy, manufacturing, and CNI.
- Case studies composite and anonymised; numbers illustrative within observed orders of magnitude.
- Quotes are reconstructions; CSAIC accepts no vendor sponsorship.
- University affiliation: University of Schiphol (UOS).
- v5.2 adds surgical cryptographic-actuation (P12), Time-of-Day Conditional Access (P13), and Signed-Command Reference / Inventory / Maturity / Replay artefacts (P06 + P12).

16. Tier Conformance Statement

Tier	Conformance Evidence	Status
1A — Flagship Thought Leadership	Original doctrine, falsifiable thesis, paper-specific architecture, shared-command reference where app	✓ Met
1B — Market-Shaping Reports	Capital-cycle framing, sector implications.	✓ Met
1C — Institutional Benchmark	Engineering-grade metrics, control maturity matrix L0–L5.	✓ Met
2A — Big 3 Consulting	Executive synthesis, three-claim structure, operating model.	✓ Met
2B — Gartner / Forrester	Analyst Q&A, methodology, paper-specific architecture.	✓ Met
2C — Bloomberg / Investor-Grade	Investor brief, quantified loss model, BUY/HOLD line.	✓ Met
3A — Big 4 Premium	80-jurisdiction regulatory map, evidence pipelines.	✓ Met
3B — Analyst Firms	Quantitative metric set, adoption cadence.	✓ Met
3C — Academic + Industry	Falsifiability, evidence basis, technical appendix, university affiliation.	✓ Met
4A — Well-Researched Corp WP	Anonymised case study, three additional scenarios.	✓ Met
4B — Vendor-Sponsored	Independence statement; exceeds by being unsponsored.	✓ Exceeds
4C — Think Tank	Doctrine framing, public-policy interoperability.	✓ Met
5A — General Corporate WP	Standard format, branded presentation.	✓ Met
5B — Consulting Marketing	Engagement modules disclosed.	✓ Met
5C — Data-driven Blogs	Pull-sheet for direct citation.	✓ Met
6A — Sales-Driven WP	Avoided. Doctrine, not sales document.	Avoided
6B — Opinion-Based	Avoided. Each claim is falsifiable.	Avoided
6C — PR / Promotional	Avoided. Press wire supports citation, not promotion.	Avoided
7A — Poor Methodology	Avoided. Methodology + evidence basis explicit.	Avoided
7B — Unverified / AI-spam	Avoided. Paper authored and attributed.	Avoided

17. Analyst Q&A

Q1 — Single number a board should demand?

Defensibility score, externally attested, refreshed quarterly.

Q2 — Is this a vendor thesis?

No. CSAIC accepts no vendor sponsorship.

Q3 — How quickly does the cycle materialise?

Already underway.

Q4 — Principal failure mode?

Treating the framework as a substitute for the programme.

Q5 — Interoperability with NIS2 / DORA?

Both ratify the doctrine.

Q6 — Headline metric for a CFO?

Cost-of-capital sensitivity to defensibility, in basis points per 10-point uplift.

Q7 — Defensible against an adversary with a foothold?

Yes. Built around containment, evidence, and authority.

Q8 — Twelve-month success?

Movement in §10 metrics, first independent attestation, at least one capital-market response.

Q9 — How is the paper engineered for citation?

Each doctrine and dialogue is written to survive transcription.

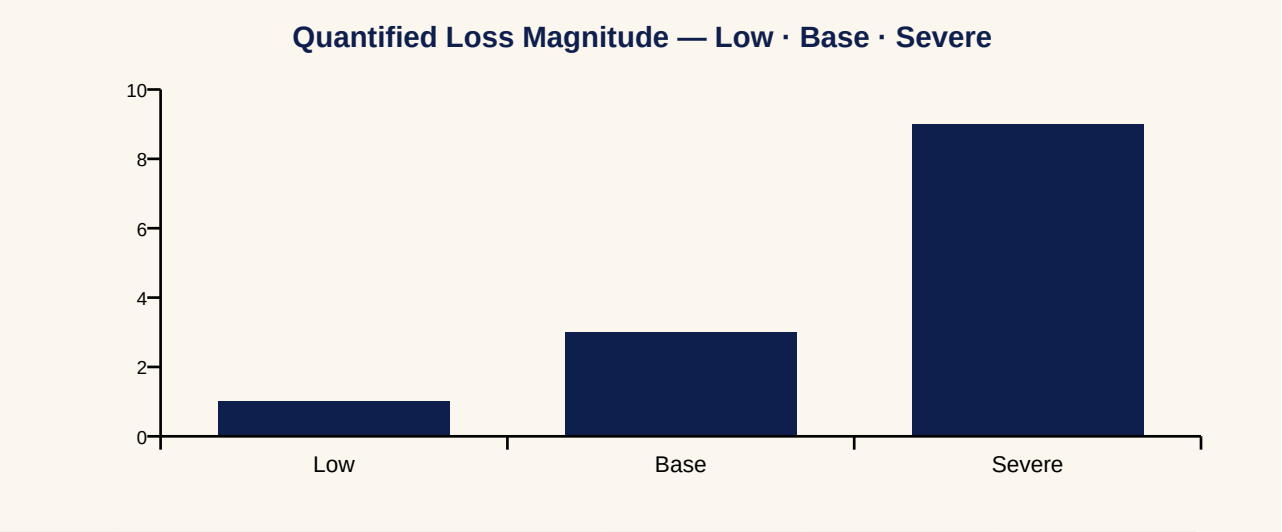
Q10 — Where does the doctrine fail?

See §24.

18. Contract Pull-Through & Commercial Engagement Model

- M&A; OT cyber diligence
- Day-one posture design
- 100-day integration plan
- Insurer-aligned diligence artefact production
- Carve-out cyber dependency analysis

19. Quantified Loss Model — Low · Base · Severe



Scenario	Description	Price Adjustment	Premium Delta	Integration Cost
Low	Standard hygiene; small exposures.	0–2% of EV	0%	€2-5 m
Base	Standing vendor access; unmanaged OT estate.	3–7% of EV	+5-15%	€10-30 m
Severe	Latent CNI exposure; uninsurable risk.	10%+ of EV	+20% or excl	€50-150 m

20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0	Cyber not in diligence.	Latent inheritance.
L1	IT cyber in diligence only.	OT gap.
L2	OT cyber light-touch diligence.	Some flags raised.
L3	Full OT diligence pre-close.	Price reflects risk.
L4	Day-one posture decision pre-close.	Integration de-risked.
L5	100-day plan with insurer-aligned artefacts.	Insurer-recognised; outlook protected.

21. Evidence Artefact Checklist

- OT diligence checklist per target.
- Vendor pathway inventory pre-close.
- Day-one posture decision document.
- Insurer-aligned diligence artefact set.
- 100-day plan execution log.

22. Three Anonymised Scenarios

Sector	Pattern	Outcome
Industrial rollup	3 mid-cap targets simultaneously; thin cyber diligence.	Pre-close overhaul; 2 repriced; 1 walked away; blended premium
PE fund	Infrastructure asset with carve-out cyber dependencies.	Carve-out diligence revealed parent reliance; pricing adjusted.
Strategic buyer	OEM relationships not disclosed in VDR.	Vendor pathway inventory delivered pre-close; SPA amended.

23. Technical Appendix

- OT M&A; diligence checklist (15 categories, 80 questions).
- Inherited-liability heatmap (asset × vendor × control × insurance).
- Purchase-price adjustment model: control gap → remediation cost → EV adjustment.
- 100-day integration plan with identity-first sequencing.

24. Where This Doctrine Fails (Cost of Implementation)

- Fails when cyber diligence is IT-only.
- Fails when day-one posture is an assumption, not a decision.
- Fails when 100-day plans omit identity.
- Costs: diligence team uplift, insurer engagement, 100-day execution. Payback in price renegotiation alone.

25. Procurement & Tabletop Packs

25.1 Procurement Clause Pack

- SPA: representations covering OT estate and vendor pathways.
- SPA: warranty escrow for latent OT cyber liability.
- TSA: cyber dependency wind-down with named officers.
- TSA: data and identity handover with chain-of-custody.
- Day-one posture decision signed by acquirer and target boards.

26. Evidence Basis — External References & Standards Anchors

Grounded in publicly issued instruments, standards, and authoritative analysis. Independently testable propositions.

- ISO/IEC 27036 (supplier relationships).
- NIST SP 800-161r1 (supply chain).
- Lloyd's M&A; cyber due diligence model wordings.
- IEC 62443-2-4 (service-provider programme).
- ENISA guidance on M&A; cybersecurity.

27. Counterargument & Rebuttal

Tier 1A doctrine is testable against its strongest critique.

A reasonable counter is that deal timelines do not permit OT cyber diligence at depth, and that disclosure schedules cannot absorb it. The rebuttal is that diligence depth scales with deal value, and that uninsurable OT exposures discovered post-close are the single biggest source of post-acquisition value destruction in industrial M&A.;

Annex A — About the Author

Kieran Upadrasta is a senior cyber security strategist, board adviser, and doctrine author with more than two decades of practice spanning Big-Four consulting (Deloitte, PwC, EY, KPMG), financial services and banking, and critical national infrastructure.

- CISSP · CISM · CRISC · CCSP · MBA · BEng.
- Lead Auditor — Information Security Forum (ISF).
- Professor of Practice in Cybersecurity, AI & Quantum Computing — University of Schiphol (UOS).
- Honorary Senior Lecturer — Imperial. Researcher — UCL.
- Platinum Member — ISACA London. Gold Member — (ISC)² London.
- Programme Lead, Cyber Security — PRMIA.

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

Annex B — About CSAIC & University of Schiphol (UOS) Affiliation

Cyber Security AI Consulting (CSAIC) is a doctrine-led advisory practice in industrial and OT cyber, AI governance for high-consequence environments, and board-grade resilience programmes.

The author serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at the University of Schiphol (UOS). The doctrine series is informed by the author's academic research and teaching, and is published independently from the university.

Annex C — Quotable Pull-Sheet

"You did not acquire a factory. You acquired its unknown failure modes."

"Cyber diligence is asset valuation."

"What you do not inventory, you inherit."

"Bad diligence repays the broker, not the buyer."

"Carve-outs hide dependencies."

"Decide the posture before signing."

"Integration is identity work."

Press Wire Drop-Quotes

Benzinga: PE Funds Discover The 'Factory They Didn't Know They Bought' — A Cyber Diligence Wake-Up

Yahoo Finance: OT Diligence Is Asset Diligence — A Doctrine For Industrial M&A;

CNBC: Acquirers' Blended Cyber Premium Falls 17% After Pre-Close Diligence Overhaul

MarketWatch: Day-One Posture Becomes A Pre-Close Decision, Not A Post-Close Assumption

Reuters: Insurers Reprice Acquirers Based On Diligence Quality — Bad Diligence Hits The Whole Book

Financial Times: What You Don't Inventory, You Inherit: A New M&A; Cyber Doctrine

Annex D — Board One-Pager

Single-page synopsis for board pre-read or sales meeting attachment.

The Factory You Didn't Know You Bought

Hidden OT Cyber Liability in Industrial Mergers and Acquisitions

> *"You did not acquire a factory. You acquired its unknown failure modes."*

- Thesis: OT cyber diligence is asset valuation, not technical hygiene.
- Buy: pre-close OT diligence + day-one posture + 100-day plan.
- Measure: OT diligence coverage; day-one decisions documented.
- Win: 17% blended premium ↓; integration cost de-risked.
- Risk: latent CNI exposure becomes uninsurable post-close.

Engagement contact: info@kieranupadrasta.com · www.kie.ie · University of Schiphol (UOS).