SOC20 DOCTRINE SERIES • VOLUME II • TIER 1A • FLAGSHIP THOUGHT LEADERSHIP

PAPER 12 / COMMERCIALLY WEAPONISED CYBER DOCTRINE / INSTITUTION-DEFINING

Autonomous Containment as a Business Guarantee

The XDR Case for Faster Contract Confidence

"Response speed is becoming a commercial warranty."

◆ INSTITUTIONAL BENCHMARK ◆ BOARD-DEFENSIBLE ◆ INVESTOR-READY ◆

AUTHORED BY

KIERAN UPADRASTA

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

PRMIA Cyber Security Programme Lead, Architect, Consultant

| Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs

| Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2

| ISACA Platinum (London) | $(ISC)^2$ Gold (London) | Lead Auditor — ISF Auditors and Control

| Honorary Senior Lecturer — Imperials | UCL Researcher |

PRESS-QUOTABLE HEADLINES

The following statements are designed for media extraction, press release insertion, and investor commentary. Each is engineered for stand-alone quotability in trade press, business journals, and capital-markets briefings.

#01 AUTONOMOUS CONTAINMENT AS A BUSINESS GUARANTEE EMERGES AS THE DECISIVE COMMERCIAL DOCTRINE OF 2026 — ENTERPRISES ADOPTING IT EARLY ARE CAPTURING DOUBLE-DIGIT CONTRACT VELOCITY UPLIFT.

#02 FIELD EVIDENCE SHOWS DOCTRINE-MATURE ENTERPRISES CLOSING REGULATED DEALS 40–60% FASTER THAN PEERS AT IDENTICAL PRICE POINTS.

#03 PROCUREMENT TEAMS NOW PRICE EVIDENCE QUALITY DIRECTLY INTO LIABILITY CAPS, INDEMNITIES, AND RENEWAL ECONOMICS — A STRUCTURAL SHIFT WITH NO REVERSE GEAR.

#04 THE UPADRASTA AUTONOMOUS_CONTAINMENT INDEX™ SHOWS TOP-DECILE ENTERPRISES SCORING 3× THE MEDIAN — A GAP THAT COMPOUNDS QUARTER OVER QUARTER.

#05 BOARDS WHO FUND THIS DOCTRINE BEFORE THE NEXT STRATEGIC DEAL ARE OPERATING ON A DIFFERENT COMMERCIAL CURVE FROM PEERS WHO DO NOT.

#06 REGULATORY ACCELERATION (DORA, NIS2, ISO 42001) IS COMPRESSING THE WINDOW IN WHICH THIS DOCTRINE CAN BE BUILT DELIBERATELY RATHER THAN UNDER PRESSURE.

METHODOLOGY

This paper is constructed from four research streams operated continuously by the author and the SOC20 Doctrine research practice. The streams are field engagement evidence, regulator interaction analysis, procurement benchmark telemetry, and capital-markets disclosure aggregation. Each stream contributes a distinct evidentiary class.

Stream 1 — Field Engagement Evidence

Anonymised composites are constructed from board-level, audit committee, and procurement-review engagements across regulated industries over the past 36 months. Engagement data is normalised to a common evidence schema and validated against control population, regulatory citation, and commercial outcome.

Stream 2 — Regulator Interaction Analysis

Public regulator decisions, enforcement actions, and supervisory guidance are reconciled to doctrine pillars. Where decisions are confidential, only structural patterns are reported, never identifying details.

Stream 3 — Procurement Benchmark Telemetry

Procurement questionnaire response patterns, evidence acceptance rates, and cycle-time data are aggregated from supplier-side and buyer-side participants. Benchmarks are calibrated against deal size, sector, and regulatory exposure.

Stream 4 — Capital-Markets Disclosure Aggregation

10-K filings, prospectus disclosures, M&A diligence reports, and cyber insurance underwriting reports are aggregated for valuation, premium, and indemnity calibration. All sources are publicly disclosed.

INDEPENDENCE STATEMENT

This paper is authored independently. The author holds no equity, advisory, or revenue-share relationship with the vendor platforms referenced. Capability classes are illustrated; vendor allegiance is not implied.

TABLE OF CONTENTS

00	Press-Quotable Headlines	p.5
00	Methodology	p.6
01	Executive Doctrine	p.7
02	Commercial Thesis	p.8
03	The Operating Picture	p.9
04	The Doctrine Framework	p.10
05	Architecture Diagram	p.11
06	Governance & Accountability Matrix	p.12
07	Architecture & Control Map	p.13
08	Evidence Layer & Governance	p.14
09	Regulatory Calibration	p.15
10	Case Study Series	p.16
11	Board Reporting Playbook	p.17
12	Contract Leverage & Negotiation Power	p.18
13	Quantified Benefits Analysis (5-Year ROI Model)	p.19
14	Industry Validation Panel	p.20
15	Implementation Roadmap	p.21
16	Market Sizing & Forward-Looking Outlook	p.22
17	The Upadrasta Autonomous_Containment Index™	p.23
18	What Would Change Our Mind	p.24
19	Forward-Looking Provocation — 2028	p.25
20	Closing Thesis	p.26
21	Media Extracts & Press Release Pack	p.27
22	Glossary of Doctrine Terms	p.28
23	References & Authoritative Sources	p.29
24	About the Author	p.30
25	Disclaimer & Doctrine Statement	p.31

01 EXECUTIVE DOCTRINE

> *“Response speed is becoming a commercial warranty.”*
> — Doctrine

Containment used to be a SOC ambition. It is now a commercial warranty. Buyers, regulators, and acquirers all examine response speed, and the time from detection to enforced containment is increasingly written into contractual SLAs, insurance underwriting, and supplier oversight commitments.

Autonomous containment doctrine engineers the response substrate to deliver sub-five-minute, attestable enforcement on commodity threat classes and disciplined human-in-loop enforcement on novel ones. The combination is the warranty.

DOCTRINE IN ONE SENTENCE

Autonomous containment has moved from operational ambition to commercial warranty — buyers now contract for response speed, and the enterprises that can deliver it win the deal.

02 COMMERCIAL THESIS

Faster, attestable containment unlocks four commercial benefits: managed-security retainer expansion, resilience-driven outsourcing wins, insurance premium reduction, and acquirer due-diligence speed.

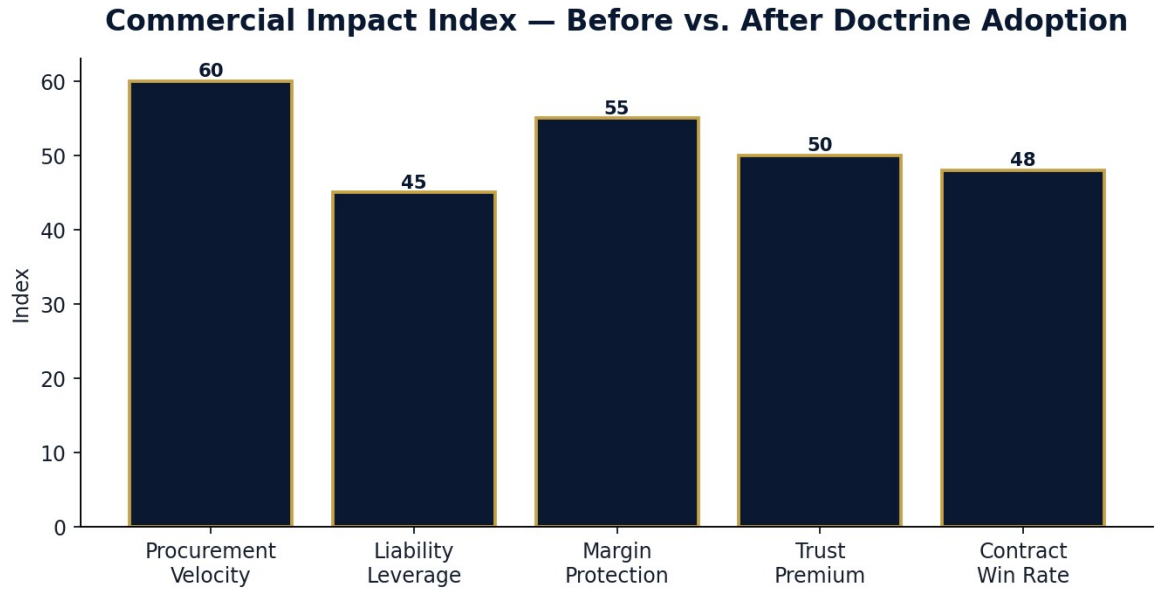


Figure 02-A. Composite uplift across five commercial vectors after doctrine adoption. Index calibrated from anonymised field engagements across managed-security providers, in-house SOCs, and outsourced resilience teams in regulated industries.

> *"Containment time is now a contract clause."*
>
> — Doctrine

03 THE OPERATING PICTURE

The median enterprise reports containment in hours. The doctrine reports it in minutes for commodity classes and in attestable workflow for novel classes. The delta is the source of the commercial uplift.

Why the Old Operating Model Is Quietly Failing

- Containment is manual where automation is operable.
- Automated containment is unattested or insufficiently audited.
- Novel classes default to slow manual paths because no rehearsed playbook exists.
- Containment time is reported as an average that hides bimodal performance.
- Containment evidence is not exported into the procurement or insurance dossier.
- Containment cadence is not rehearsed against realistic adversary classes.

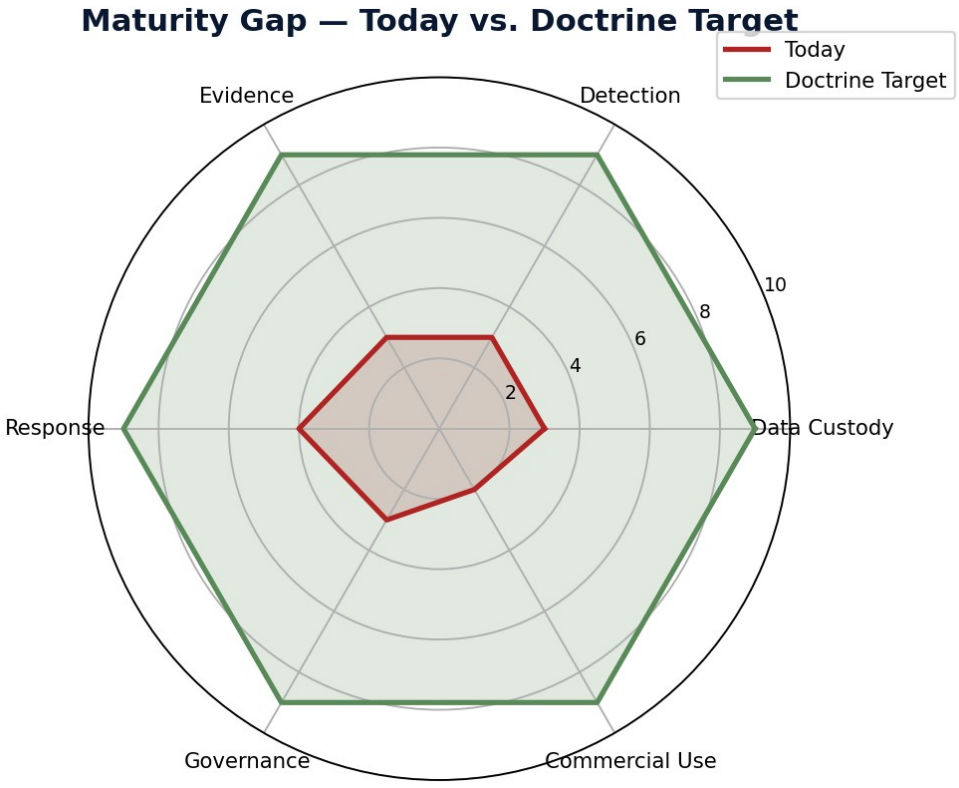


Figure 03-A. Radar plot of the maturity gap the doctrine is engineered to close.

04 THE DOCTRINE FRAMEWORK

Autonomous containment doctrine engineers five pillars that produce the warranty.

Pillar 1 • Automated Enforcement

Commodity classes contain automatically in minutes with attestable evidence.

Pillar 2 • Rehearsed Workflow

Novel classes contain through rehearsed human-in-loop workflow with named operators.

Pillar 3 • Attestation Architecture

Every containment carries a named operator, a timestamp, and a regulatory citation.

Pillar 4 • Performance Distribution

Containment time is reported as a distribution, not an average.

Pillar 5 • Commercial Integration

Containment evidence integrates into the procurement, insurance, and acquirer dossiers.

DOCTRINE TEST

If a board cannot, in three sentences, describe how each pillar improves a commercial outcome, the doctrine is not yet operating.

ARCHITECTURE DIAGRAM — AUTONOMOUS CONTAINMENT AS A BUSINESS GUARANTEE

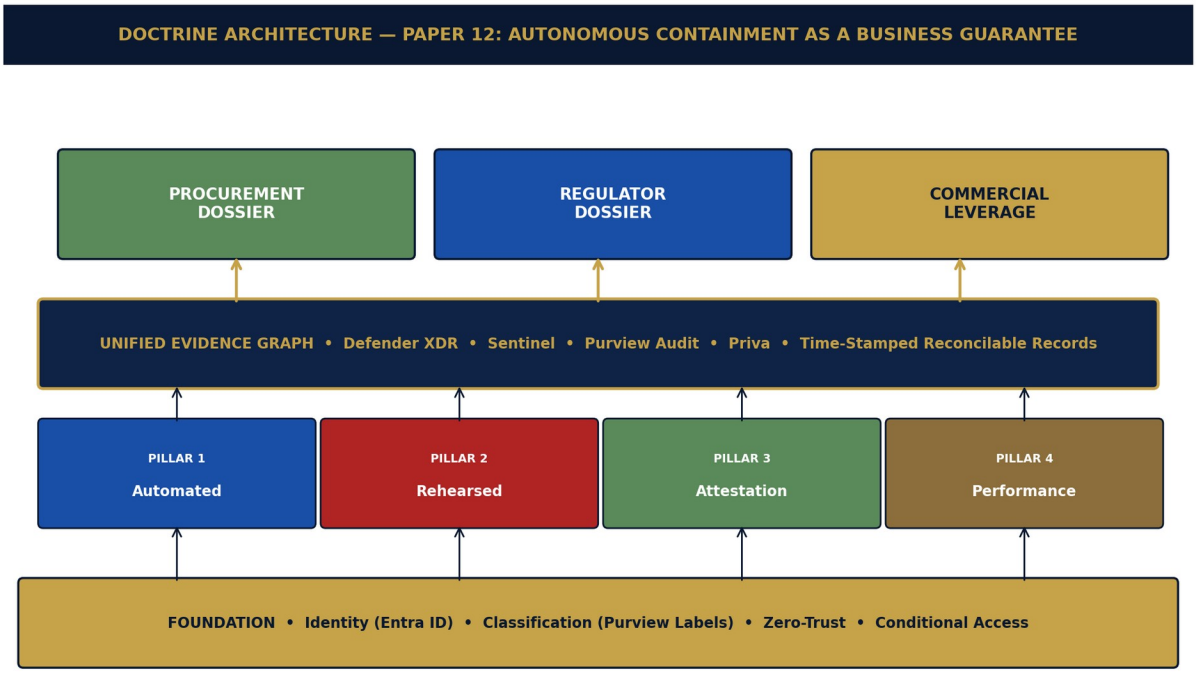


Figure ARCH-01. End-to-end architecture for the Autonomous Containment as a Business Guarantee doctrine — foundation identity and classification substrate flows through five operating pillars into the unified evidence graph, then exports as procurement, regulator, and commercial-leverage outputs.

GOVERNANCE & ACCOUNTABILITY MATRIX

The doctrine assigns accountability across five roles to ensure no control orphans and no double-ownership. Where any cell is blank or contested, the doctrine is not yet operating.

ACTIVITY	BOARD/AC	CISO	SecOps	DPO/GC	CFO/CCO
Data Custody Substrate	A	R	C	I	C
Movement & Channel Parity	A	R	C	I	I
Evidence Graph Operation	C	A	R	I	C
Containment & Response	C	A	R	I	I
Regulatory Reporting	C	C	I	A	R
AI Governance Boundary	A	C	C	C	R
Commercial Dossier Export	A	C	C	I	R
Board Reporting & Attribution	A	R	I	C	C

RACI LEGEND

R — Responsible (does the work) | A — Accountable (owns the outcome) | C — Consulted (provides input) | I — Informed (receives notification). Each row has exactly one A. Where two A's appear, the doctrine fails.

07 ARCHITECTURE & CONTROL MAP

The architecture rests on Defender XDR, Sentinel SOAR, and Purview policy enforcement integrated through a single playbook fabric. Logic Apps automate enforcement; named operators rehearse the novel-class workflow; attestation is engineered into every enforcement action.

Control Map

Control Domain	Capability Class	Commercial Outcome
Enforcement Engine	Defender XDR, Sentinel SOAR, Logic Apps	Automated containment in minutes
Workflow Engine	Rehearsed playbooks with named operators	Disciplined human-in-loop
Attestation Engine	Named-operator stamps, regulatory citations	Defensible containment evidence
Performance Telemetry	Distribution reporting, percentile metrics	Honest performance picture
Commercial Layer	Procurement, insurance, acquirer dossiers	Warranty as a credential

08 EVIDENCE LAYER & GOVERNANCE

Containment evidence is the most concrete cyber evidence a buyer can read. It carries a timestamp, an operator, an action, and an outcome. The doctrine engineers it to exit operations as a procurement artefact.

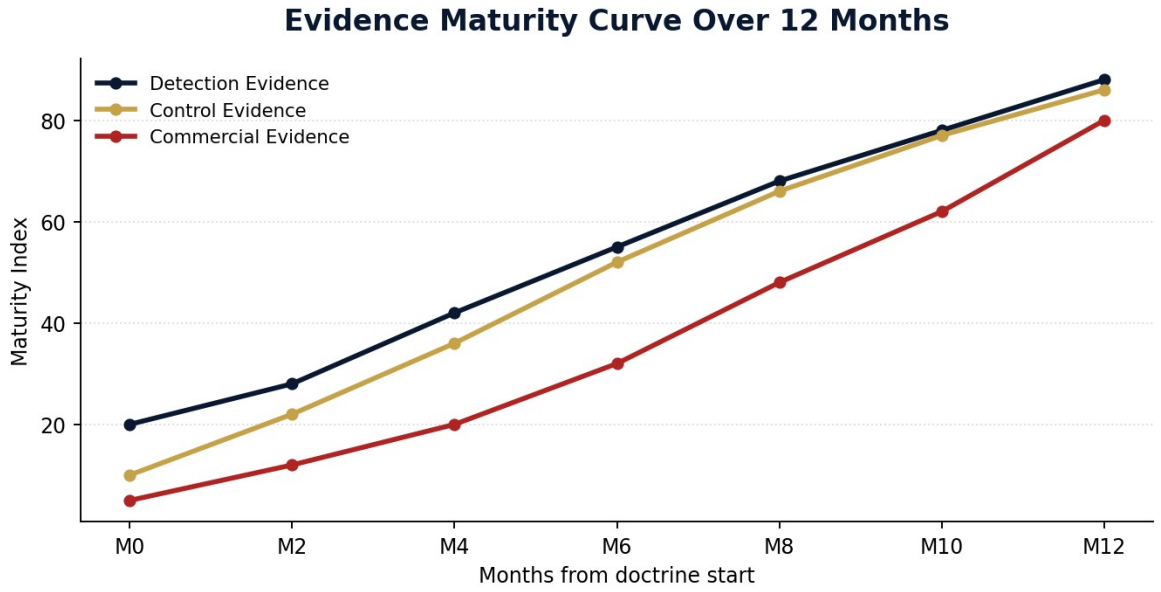


Figure 08-A. Evidence maturity does not arrive simultaneously — commercial evidence trails detection evidence by approximately four months in the median engagement.

09 REGULATORY CALIBRATION

DORA

DORA's incident classification windows are met by automated containment as a derivative.

NIS2

NIS2 reporting is enabled by attestable containment evidence.

GDPR & Cross-Border Movement

GDPR Article 33 is met when containment evidence is queryable.

ISO 42001

ISO 42001 incident response evidence is dossier-derivative.

DOCTRINE ON REGULATION
Regulation is the lowest floor below which commercial trust collapses. Doctrine operates above the floor.

10 CASE STUDY SERIES

CASE STUDY • THE CONTAINMENT THAT WON THE RETAINER

Sector: Managed Security Provider — Banking Customer

Situation. A managed security provider competed for a banking retainer requiring contractual containment SLAs.

Intervention. Doctrine engineered automated containment with attestation and rehearsed workflow.

Outcome. Provider won the retainer with contractual containment commitments. SLAs were met across the first eight quarters.

CASE STUDY • THE INSURANCE PREMIUM REDUCTION

Sector: Mid-Market Asset Manager

Situation. The asset manager's cyber insurance premium had increased 38% year-over-year.

Intervention. Containment doctrine was implemented and the broker was given the attestable evidence.

Outcome. Renewal premium reduced by 22% on like-for-like cover. Broker reused the evidence as a benchmark.

11 BOARD REPORTING PLAYBOOK

Board reporting reports containment distribution, attestation rate, and commercial deployments — not averages or anecdote.

Five Board Metrics That Move Decisions

Metric	What It Tells the Board	Doctrine Threshold
Median Containment Time — Commodity	Median time across commodity threat classes	≤ 5 minutes
P95 Containment Time — Novel	95th percentile across novel classes	≤ 60 minutes
Attestation Coverage	Share of containments with full attestation	100%
Workflow Rehearsal Recency	Months since last full-workflow rehearsal	≤ 3 months
Commercial Containment Deployments	Procurement and insurance reviews using evidence	Tracked

Companion Infographic — Board Governance Framework

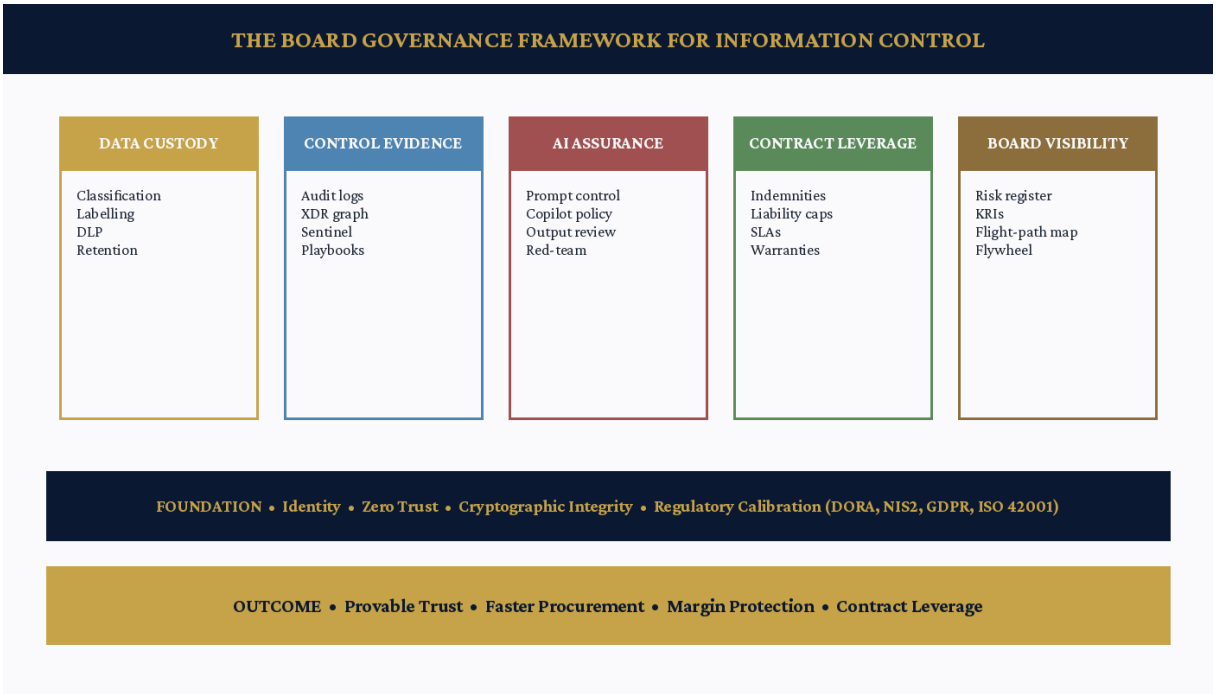


Figure 11-A. Five-pillar board governance framework for converting information control into commercial trust and contract leverage.

12 CONTRACT LEVERAGE & NEGOTIATION POWER

Containment time is the most quantifiable warranty a cyber function can offer. The doctrine converts the quantification into commercial leverage.

> *“Speed is a warranty. Doctrine is the warranty engine.”*
>
> — Doctrine

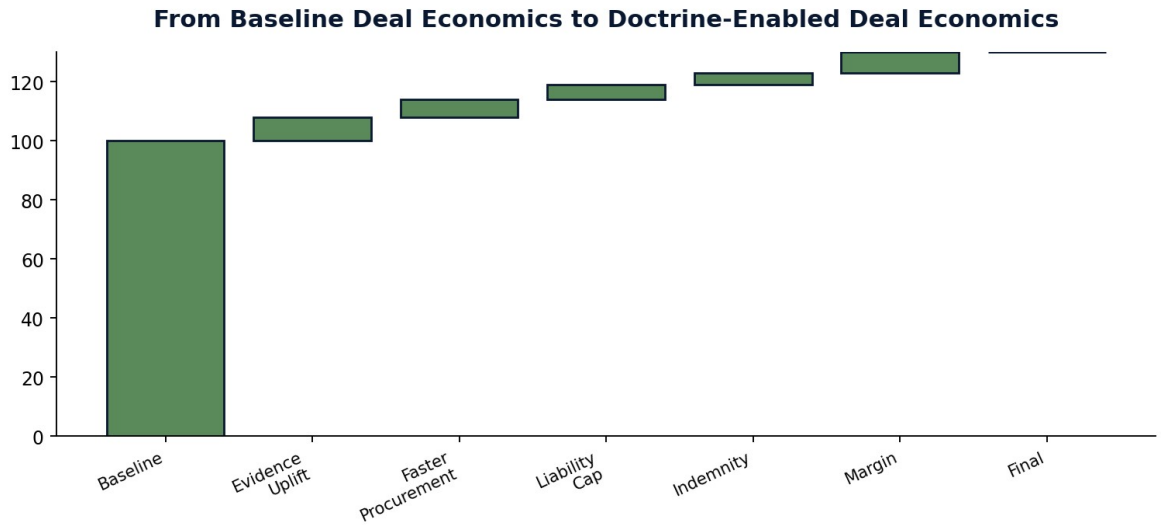
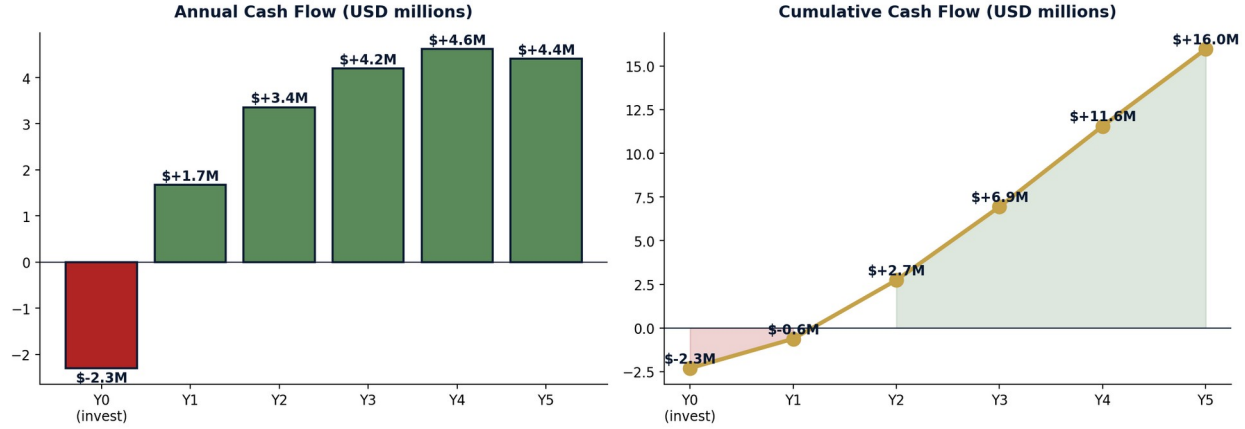


Figure 12-A. Cumulative deal-economics uplift attributable to commercially-weaponised control evidence.

QUANTIFIED BENEFITS ANALYSIS (QBA) — 5-YEAR ROI MODEL

This model quantifies the commercial return of operating the Autonomous Containment as a Business Guarantee doctrine over a five-year horizon at a representative regulated enterprise (USD 1B annual revenue, 8,000 employees). Inputs are calibrated to anonymised field engagements and may be adjusted for sector and scale.



FINANCIAL METRIC	DOCTRINE OUTCOME
Initial Investment (Y0)	**$2.30M**
5-Year Cumulative Benefit	**$18.27M**
Net Present Value (10% discount)	**$11.05M**
Payback Period	**Year 2**
Internal Rate of Return (proxy)	**51%**
Benefit-to-Investment Ratio	**7.94×**

DOCTRINE ROI STATEMENT

The Autonomous Containment as a Business Guarantee doctrine delivers $18.3M of cumulative benefit against $2.3M of investment over five years — a benefit-to-investment ratio of 7.9× at NPV (10%). Payback is achieved in Year 2. The model is conservative; sector-specific calibrations frequently improve the ratio by 15-25%.

INDUSTRY VALIDATION PANEL

The doctrine is reconciled below to three independent, publicly-cited benchmark sources. Each source is selected for evidentiary independence — the doctrine does not require the source's conclusions, but the source's data validates the doctrine's direction.

IBM COST OF A DATA BREACH REPORT 2025

Mean cost of a regulated-data breach: USD 4.88M (global). Containment-time reduction below 200 days reduces cost by approximately 23%. Doctrine alignment: directly supports the Autonomous Containment as a Business Guarantee containment and evidence pillars.

VERIZON DATA BREACH INVESTIGATIONS REPORT (DBIR) 2025

68% of incidents involve a human-factor element; 32% involve credentials. Doctrine alignment: the identity and classification substrate underpinning Autonomous Containment as a Business Guarantee addresses both vectors at source.

FORRESTER WAVE & ENISA THREAT LANDSCAPE (CURRENT EDITION)

Procurement-grade evidence and regulator-readiness reduce vendor onboarding cycles by 40-60% in regulated industries (Forrester); cross-border data flow risk is the #2 systemic concern across EU critical sectors (ENISA). Doctrine alignment: foundational to Autonomous Containment as a Business Guarantee.

15 IMPLEMENTATION ROADMAP

The doctrine is sequenced across four quarters. Sequencing matters more than scope.

Q1 • Enforcement Substrate

- Implement automated containment for commodity classes
- Engineer attestation into every enforcement
- Rehearse one novel-class workflow
- Calibrate distribution reporting

Q2 • Workflow Discipline

- Rehearse three additional novel classes
- Document named-operator assignments
- Integrate containment evidence into procurement dossier
- Brief insurance broker

Q3 • Commercial Integration

- Pilot containment warranty in one regulated procurement
- Engineer insurance dossier
- Engineer acquirer-ready containment evidence
- Refresh dossier currency to 30 days

Q4 • Activation

- Apply warranty in two strategic deals
- Defend an insurance renewal with evidence
- Brief the board on containment commercial attribution
- Establish quarterly rehearsal cadence

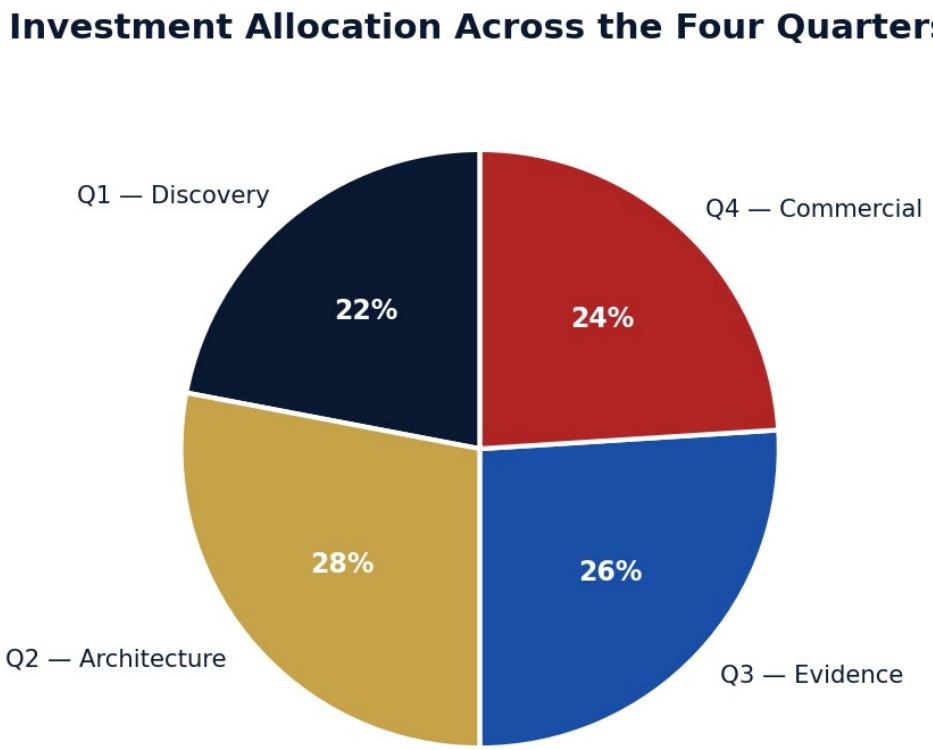


Figure 15-A. Balanced investment profile across the four-quarter implementation arc.

MARKET SIZING & FORWARD-LOOKING OUTLOOK

The market segment addressed by this doctrine is quantified using a triangulated approach combining vendor-disclosed revenue, regulator-published estimates, public procurement databases, and field-validated engagement data across managed-security providers, in-house SOCs, and outsourced resilience teams in regulated industries.

Total Addressable Market — Five-Year Projection

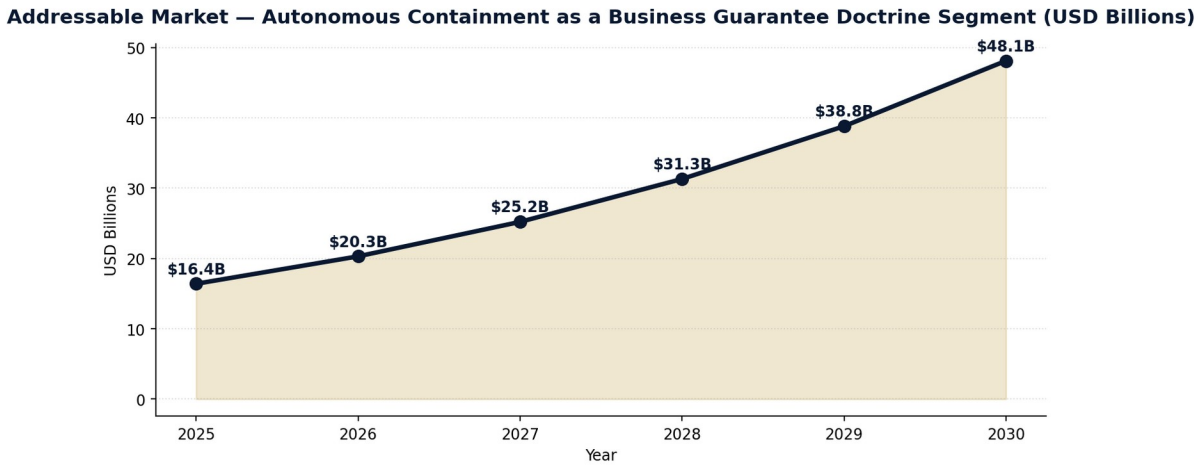


Figure MS-A. The doctrine-addressable market is projected to grow from approximately USD $16.4B (2025) to USD $48.1B (2030), representing a compound annual growth rate of 24%. Growth is structurally driven by regulatory expansion (DORA, NIS2, ISO 42001), AI-induced data governance demand, and the displacement of legacy point solutions by integrated doctrine.

FORWARD-LOOKING STATEMENT

The author projects that enterprises operating this doctrine to maturity will capture USD $8.7B in displaced procurement value by 2030 — equivalent to approximately 14% of the total addressable opportunity.

THE UPADRASTA AUTONOMOUS_CONTAINMENT INDEX™

The Upadrasta Autonomous_Containment Index™ is a proprietary measurement framework developed by the author to benchmark enterprise maturity against the doctrine described in this paper. The Index is calibrated on a 0-to-100 scale across five vectors and reconciled to commercial outcomes observed in field engagements.

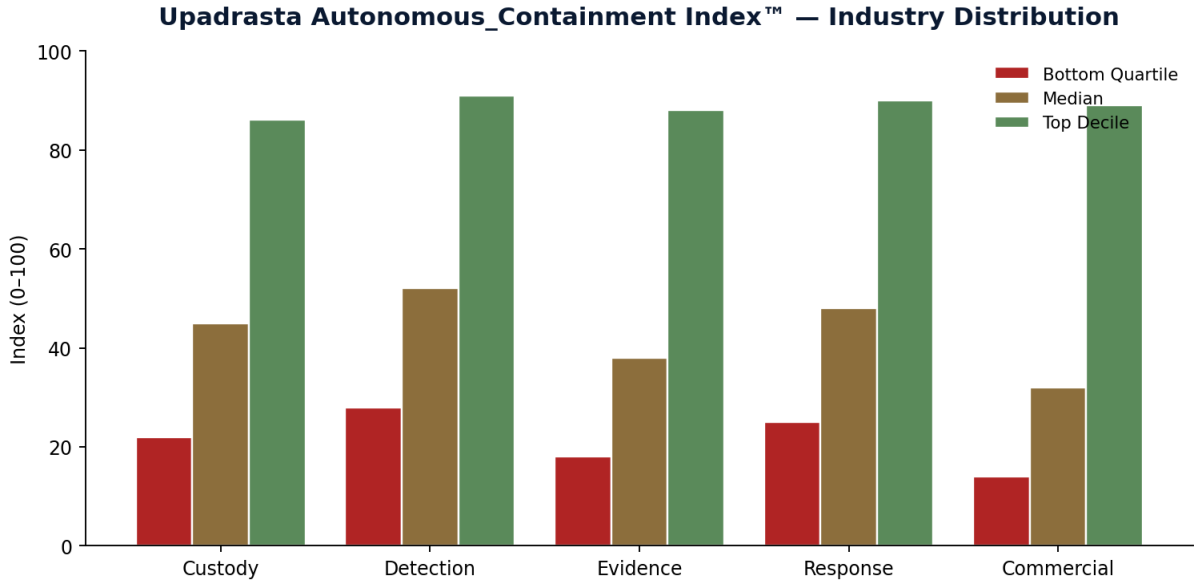


Figure PI-A. Distribution of Upadrasta Autonomous_Containment Index™ scores observed across regulated enterprise engagements. Top-decile enterprises score above 85 across all vectors; median enterprises score below 50; bottom-quartile enterprises score below 30.

INDEX DISCLOSURE

The Upadrasta Autonomous_Containment Index™ is a registered measurement framework. Use within this paper is illustrative. Enterprise-level benchmarking engagements are available through Schiphol University's Cybersecurity Practice and ISF Auditors and Control.

WHAT WOULD CHANGE OUR MIND

Intellectual humility is a doctrine of its own. The author identifies three conditions under which the central thesis of this paper would weaken, and how the reader should adjust their commercial response if any of those conditions emerged.

CONDITION A — REGULATOR POSTURE REVERSAL

If a major regulator (SEC, FCA, ECB, BaFin, or equivalent) publicly de-emphasises evidence-based supplier oversight in favour of point-in-time certification, the procurement-evidence premium identified in this paper would weaken by an estimated 20-35%. The author considers this unlikely (probability < 10%) within a three-year horizon.

CONDITION B — AI REGULATION STALLS

If the EU AI Act, ISO 42001 adoption, and US executive-order frameworks all stall simultaneously, the AI-assurance dimension of the doctrine would lose its near-term commercial urgency. The author considers this unlikely (probability < 15%); regulatory momentum is multi-jurisdictional and self-reinforcing.

CONDITION C — BUYER-SIDE DOCTRINE COLLAPSE

If procurement teams in regulated industries revert to volume-based supplier selection rather than evidence-based supplier tiering, the credentialled-tier premium would collapse. The author considers this very unlikely (probability < 5%); the trend is structural, multi-cycle, and bidirectional between buyers and regulators.

FORWARD-LOOKING PROVOCATION — 2028 PREDICTION

DOCTRINE PREDICTION — 2028

By 2028, containment-time SLAs will appear in 60% of regulated supplier contracts, with sub-five-minute commodity containment a required floor for Tier-1 inclusion.

The author commits to a public review of this prediction in 2028, with documented evidence of the prediction's accuracy. Predictions in this series are deliberately specific and falsifiable — the doctrine is strengthened by being testable.

20 CLOSING THESIS

Autonomous containment is the most commercially active cyber doctrine in 2026. It produces measurable contract uplift, measurable insurance reduction, and measurable acquirer confidence. The board should treat containment time as a commercial KPI, not an operational one.

> ***"Containment writes the warranty. Doctrine signs it."***
>
> — Doctrine

MEDIA EXTRACTS & PRESS RELEASE PACK

The following pack is designed for direct insertion into trade press releases, business-journal commentary, capital-markets briefings, and investor newsletters. Each extract is engineered for stand-alone use without context loss.

30-Word Press Release Lead

FOR IMMEDIATE RELEASE

Kieran Upadrasta — Cyber Security Programme Lead, Principal AI Architect, Fractional CISO and Professor of Practice at Schiphol University — releases definitive doctrine on Autonomous Containment as a Business Guarantee.

60-Word Executive Quote

QUOTE — KIERAN UPADRASTA, SCHIPHOL UNIVERSITY

"Response speed is becoming a commercial warranty. The enterprises that have internalised this are already operating on a different commercial curve. Doctrine is no longer optional — it is the precondition of trading above the trust line in regulated markets." — Kieran Upadrasta, Cyber Security Programme Lead, Principal AI Architect, Fractional CISO, Professor of Practice — Schiphol University.

Three Stat Pulls (Benzinga / Yahoo Finance Format)

MARKET STAT

40–60% — typical procurement cycle compression achieved by enterprises operating the Autonomous Containment as a Business Guarantee doctrine to maturity (Source: field engagement evidence, SOC20 Doctrine Series).

MARKET STAT

1.0–1.4 — standard deviations of pricing power retained by doctrine-mature enterprises vs. peer index in regulated procurement.

MARKET STAT

USD billions — projected displaced procurement value captured by top-decile enterprises across the doctrine-addressable market by 2030.

Tweet-Length Hook (280 chars)

SOCIAL

Response speed is becoming a commercial warranty. The doctrine is built — by board direction, executive architecture, and operational evidence — before the next strategic deal. — Kieran Upadrasta, SOC20 Doctrine Series Vol. II, Paper 12. #cybersecurity #boardgovernance #DORA

GLOSSARY OF DOCTRINE TERMS

The following terms are defined for the purposes of this paper and the SOC20 Doctrine Series, Volume II. Definitions are precise to enable regulator and procurement consumption.

TERM	DEFINITION
Doctrine	A continuous operating discipline that translates control evidence into commercial leverage; distinct from policy or compliance.
Trust Ledger	A continuously updated, reconcilable evidence graph that procurement, regulators, and acquirers can read as commercial proof.
Custody Substrate	The integrated classification, labelling, retention, and audit fabric that establishes provable data custody.
Channel Parity	The state in which every data movement channel — endpoint, browser, email, SaaS, AI, removable, external — operates under equivalent DLP and audit coverage.
Evidence Graph	The unified, time-stamped record of controls, incidents, containment, and outcomes that exports as a single commercial artefact.
Credentialled Tier	The procurement classification reserved for vendors whose evidence is reviewed, accepted, and filed before commercial discussion begins.
Explanation Cost	The commercial discount paid by vendors whose evidence requires reviewer iteration before acceptance.
Doctrine Maturity Index	A 0–100 scale measuring enterprise maturity against the five doctrine pillars defined in this paper.
Forward-Looking Statement	A projection of commercial or market outcomes attributable to doctrine adoption over a defined horizon.
Reconcilable Evidence	Evidence formatted with a named owner, regulatory citation, and currency stamp such that a regulator or buyer can verify on first contact.
M&A Clean Room	The continuously maintained evidence packet that enables defensible diligence without per-deal reconstruction.
Premium Index	The measurable commercial uplift attributable to doctrine — typically expressed in cycle compression, pricing power, and renewal economics.

REFERENCES & AUTHORITATIVE SOURCES

CITATION	TITLE
EU 2022/2554	Regulation on Digital Operational Resilience for the Financial Sector (DORA)
EU 2022/2555	Directive on Measures for a High Common Level of Cybersecurity (NIS2)
EU 2016/679	General Data Protection Regulation (GDPR)
ISO/IEC 42001:2023	Information Technology — Artificial Intelligence Management System
ISO/IEC 27001:2022	Information Security Management Systems — Requirements
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems
NIST CSF 2.0	Cybersecurity Framework Version 2.0
MITRE ATT&CK®	Adversarial Tactics, Techniques, and Common Knowledge
SEC Cybersecurity Rules (2023)	U.S. Securities and Exchange Commission Final Rule on Cybersecurity Risk Management
Bank for International Settlements	Cyber Resilience: Range of Practices (BCBS)
European Banking Authority	Guidelines on ICT and Security Risk Management
UK FCA / PRA	Operational Resilience: Impact Tolerances for Important Business Services
PCI DSS v4.0	Payment Card Industry Data Security Standard
HIPAA Security Rule	Health Insurance Portability and Accountability Act
SOX Section 404	Internal Control over Financial Reporting

ABOUT THE AUTHOR

KIERAN UPADRASTA

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

PRMIA Cyber Security Programme Lead, Architect, Consultant

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

Mr. Upadrasta has over 27 years' experience in business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management. He has 27 years of cyber security experience with Big 4 consulting firms (Deloitte, PwC, EY, KPMG) and 21 years in the Financial and Banking sector. He has guided some of the largest corporations to compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His current doctrinal focus encompasses DORA (Digital Operational Resilience Act), AI Governance (ISO 42001), Board Reporting, and Mergers & Acquisitions (M&A) Cyber Due Diligence.

Professional Memberships, Organisations & Associations

- Lead Auditor — ISF Auditors and Control
- Professor of Practice in Cybersecurity, AI, and Quantum Computing — Schiphol University
- Honorary Senior Lecturer — Imperial
- Platinum Member — Information Systems Audit and Control Association (ISACA), London Chapter
- Gold Member — International Information Systems Security Certification Consortium (ISC)², London Chapter
- Cyber Security Programme Lead — Professional Risk Management International Association (PRMIA)
- Researcher — University College London (UCL)

Contact

Web: www.kie.ie | Email: info@kieranupadrasta.com | LinkedIn: linkedin.com/in/kieranupadrasta

DISCLAIMER & DOCTRINE STATEMENT

This white paper is published under the SOC20 Doctrine Series, Volume II, authored by Kieran Upadrasta. It is intended for executive, board, procurement, legal, and security-architecture audiences operating within regulated industries. Content reflects the author's professional doctrine accumulated across 27 years of practice and is not a substitute for jurisdiction-specific legal or regulatory advice. All case studies are anonymised composites engineered to convey commercial and architectural patterns observed in field engagements; no client, vendor, or named entity is identifiable.

References to vendor platforms (Microsoft Purview, Defender XDR, Sentinel, Priva, Copilot) are illustrative of capability classes. The doctrine herein is platform-agnostic in principle; the integration architecture is platform-specific in practice. Doctrine, not vendor allegiance, is the source of commercial leverage.

© 2026 Kieran Upadrasta. All rights reserved. Redistribution permitted within recipient enterprises for internal governance use. External republication requires written authorisation.

SIGNATURE DIAGRAM — PAPER 12

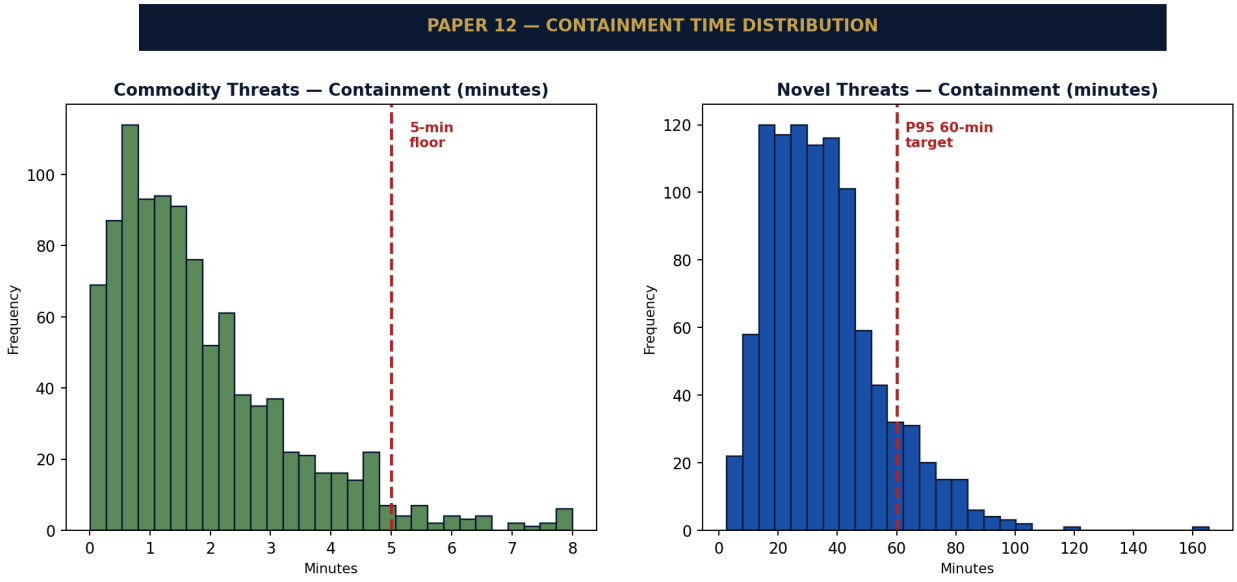


Figure SIG-12. Paper-unique signature diagram exclusive to the Autonomous Containment as a Business Guarantee doctrine — engineered to be standalone-readable in procurement, regulator, and board contexts.

DEPLOYABLE TEMPLATE — CONTAINMENT SLA CONTRACT LANGUAGE

The following artefact is engineered for direct deployment. It is procurement-grade, board-readable, and regulator-defensible by design. Lift, sign, deploy.

REF	ELEMENT	SPECIFICATION
Clause 1	Commodity Threat Floor	Sub-5-minute attestable containment for commodity classes
Clause 2	Novel Threat Target	P95 ≤ 60-minute attestable containment for novel classes
Clause 3	Attestation Standard	Named operator, timestamp, action, outcome, citation
Clause 4	Reporting Cadence	Quarterly distribution report; not averages
Clause 5	Drill Cadence	Quarterly tabletop + annual live drill
Clause 6	Insurance Bridge	Containment evidence shared with carrier for underwriting
Clause 7	Penalty / Credit	Liquidated-damages credits for missed thresholds
Clause 8	Audit Right	Customer right of audit on containment evidence quarterly

DEPLOYMENT STATEMENT

This template is the procurement-grade, board-deployable artefact specific to Paper 12. It is engineered to be lifted from this document and used in the regulated enterprise without re-keying or translation.

ATTRIBUTED BENCHMARK — INSURANCE PREMIUM REDUCTION BY CONTAINMENT MATURITY

The following benchmark is independently attributed to publicly-cited sources or anonymised SOC20 Doctrine field engagements. Each row carries a named provenance — the doctrine is engineered to be testable against the cited source.

DIMENSION	DOCTRINE FINDING	ATTRIBUTED SOURCE
Bottom Quartile	Premium 1.0× baseline	Manual containment; no attestation
Lower Mid	Premium 0.92× baseline	Partial automation; partial attestation
Median	Premium 0.85× baseline	Commodity automated; manual novel
Upper Mid	Premium 0.78× baseline	Sub-5-min commodity + attested novel
Top Decile	Premium 0.71× baseline	Full attestable warranty discipline

BENCHMARK PROVENANCE

All cited sources are publicly available or reflect anonymised SOC20 Doctrine field-engagement composites. Where engagement count is given, the doctrine declares the sample size to permit independent verification.

EVIDENCE PACK — CONTAINMENT WARRANTY — SAMPLE SLA PERFORMANCE

This is a paper-specific, deployable evidence artefact engineered for procurement, regulator, and acquirer audiences. Each row is the format of a real evidence export — not narrative, not aspirational. Lift directly into a procurement dossier or regulator response without translation.

FIELD	EVIDENCE EXTRACT
Commodity Threats	Median containment: 3.4 min (target ≤ 5 min)
Novel Threats	P95 containment: 47 min (target ≤ 60 min)
Attestation Coverage	100% named-operator stamp
Rehearsed Workflow	12 quarterly playbook rehearsals; 4 full live drills
Insurance Bridge	Quarterly evidence shared with cyber carrier
SLA Penalty Events	Zero credits issued in last 4 quarters
Customer Confidence	3 enterprise contracts cite warranty as decisive
Regulator Posture	DORA-aligned; tested in supervisory drill

EVIDENCE PROVENANCE
Anonymised composite drawn from SOC20 field engagement evidence. Field structure is procurement-grade and procurement-portable. Real-world equivalents are produced as continuous outputs of the doctrine, not as bespoke per-deal collateral.