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

PAPER 16 / COMMERCIALLY WEAPONISED CYBER DOCTRINE / INSTITUTION-DEFINING

Automated Defence, Auditable Outcomes

Making Sentinel Playbooks Board-Defensible

"Automation without evidence is speed without accountability."

◆ 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 |

CONFIDENTIAL • EXECUTIVE-GRADE • BOARD-DEFENSIBLE • PRESS-READY • INVESTOR-GRADE

Version 1.0 • May 2026 • www.kie.ie • info@kieranupadrasta.com • ISBN-style edition: SOC20-VII-16

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 AUTOMATED DEFENCE, AUDITABLE OUTCOMES 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 AUTOMATED_DEFENCE 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

01 EXECUTIVE DOCTRINE

> *"Automation without evidence is speed without accountability."*
>
> — Doctrine

Sentinel SOAR, Logic Apps, and orchestrated playbooks are the most operationally valuable automation substrate available to regulated security operations. They are also the most under-evidenced. The doctrine in this paper closes the evidence gap and converts operational acceleration into board-defensible commercial value.

Automation without audit evidence is operational speed at the cost of accountability. Doctrine demands both. Every automated action must produce attestable, named, and citable evidence at the point of enforcement.

DOCTRINE IN ONE SENTENCE

Automation accelerates response, but only audit evidence converts the acceleration into board-defensible commercial value.

02 COMMERCIAL THESIS

Audit-grade automation produces three commercial outcomes: regulator confidence in operational resilience, procurement-grade evidence of response speed, and insurance underwriting evidence that compresses premium calculation.

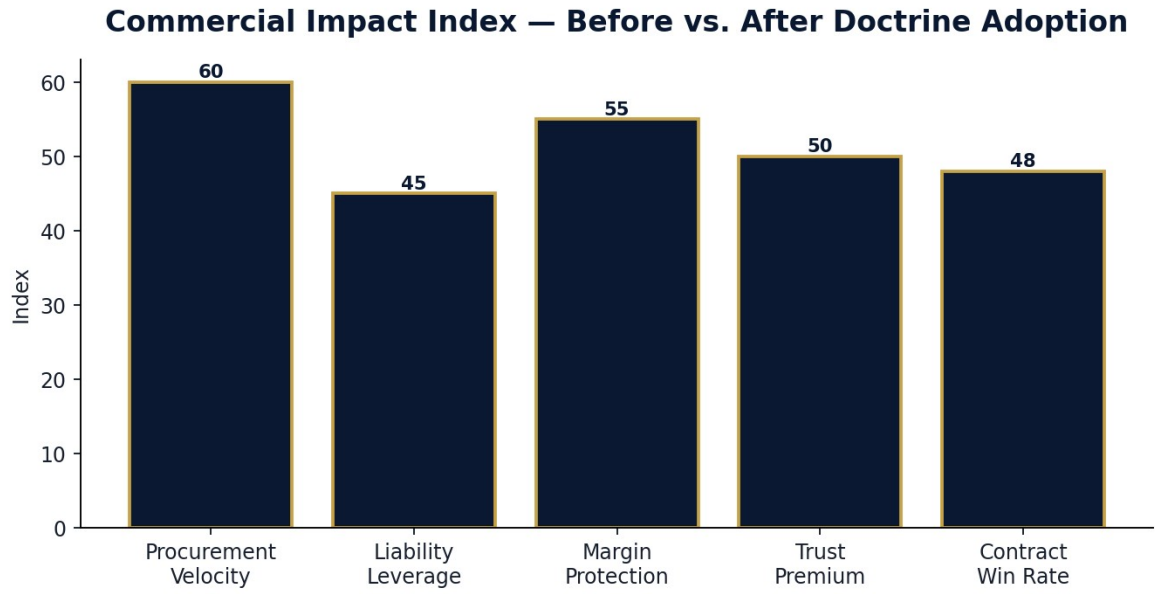


Figure 02-A. Composite uplift across five commercial vectors after doctrine adoption. Index calibrated from anonymised field engagements across regulated enterprises operating Sentinel SOAR and Logic Apps automation in their security operations.

> *"Automation is the fastest path to speed and the slowest path to trust unless evidence is engineered into it."*
>
> — Doctrine

03 THE OPERATING PICTURE

The median Sentinel automation deployment runs 18–40 playbooks with limited audit instrumentation. Playbook outcomes are visible in operational logs but absent from procurement, regulator, and insurance dossiers. The acceleration value is captured operationally; the commercial value is forfeited.

Why the Old Operating Model Is Quietly Failing

- Playbooks act without attestable, named-operator evidence.
- Logic Apps run unaudited steps that the regulator cannot reconstruct.
- Containment automation has no named control owner.
- Playbook performance is not measured against a value definition.
- Audit logs are not exported into the dossier.
- Playbook libraries grow without periodic curation.

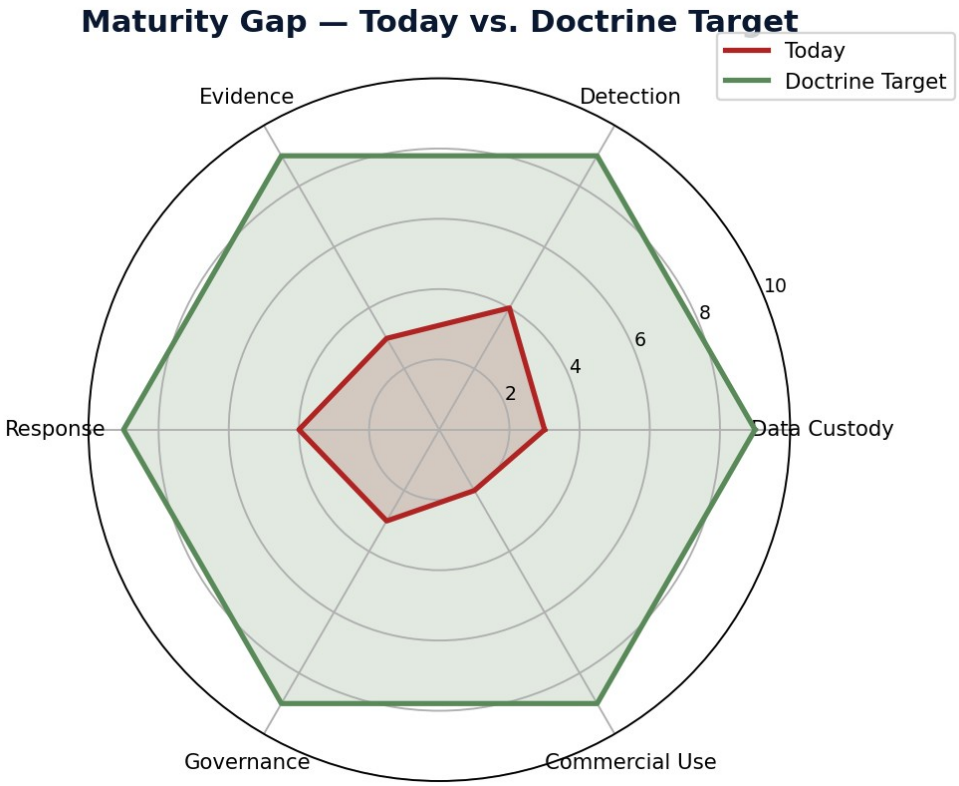


Figure 03-A. Radar plot of the maturity gap the doctrine is engineered to close.

04 THE DOCTRINE FRAMEWORK

Audit-grade automation doctrine engineers five pillars that make automation defensible.

Pillar 1 • Attestable Actions

Every automated action produces named-operator, timestamped, citable evidence.

Pillar 2 • Reconstructable Workflow

Logic Apps and SOAR sequences are reconstructable for regulators.

Pillar 3 • Ownership Architecture

Each playbook has a named owner accountable to the board.

Pillar 4 • Value Calibration

Playbook performance is measured against a documented value definition.

Pillar 5 • Curation Discipline

Playbook libraries are curated quarterly for currency and value.

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 — AUTOMATED DEFENCE, AUDITABLE OUTCOMES

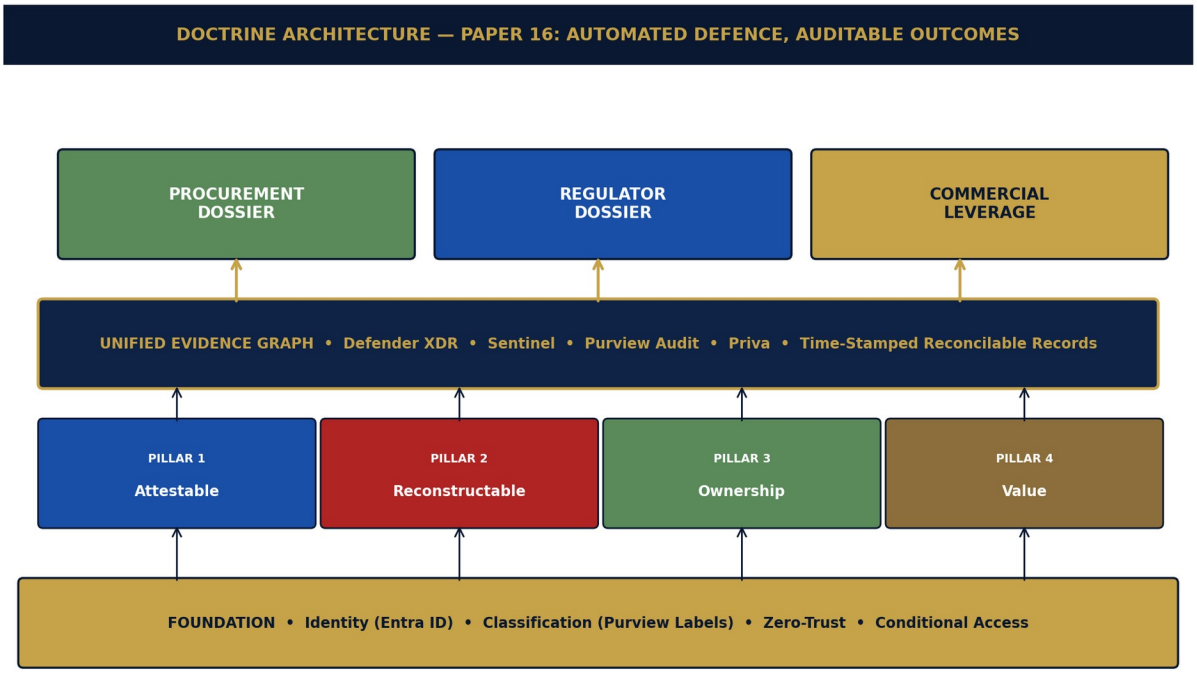


Figure ARCH-01. End-to-end architecture for the Automated Defence, Auditable Outcomes doctrine — foundation identity and classification substrate flows through five operating pillars into the unified evidence graph, then exports as procurement, regulator, and commercial-leverage outputs.

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 Sentinel SOAR, Logic Apps, Defender XDR enforcement APIs, and the Purview audit substrate. Logic Apps are engineered with audit logging at every step. Outputs flow into the unified evidence graph.

Control Map

Control Domain	Capability Class	Commercial Outcome
Action Layer	Logic Apps audit, attestation tagging	Defensible enforcement evidence
Workflow Layer	SOAR step reconstruction, audit trail	Regulator-readable workflow
Ownership Layer	Named owners per playbook	Board-accountable automation
Calibration Layer	Value definitions per playbook	Performance honesty
Curation Layer	Quarterly library review	Living automation library

08 EVIDENCE LAYER & GOVERNANCE

Audit-grade automation evidence is engineered into the procurement and regulator dossier. Every playbook contributes evidence that the regulator can read in the same format as the SOC reads operational logs.

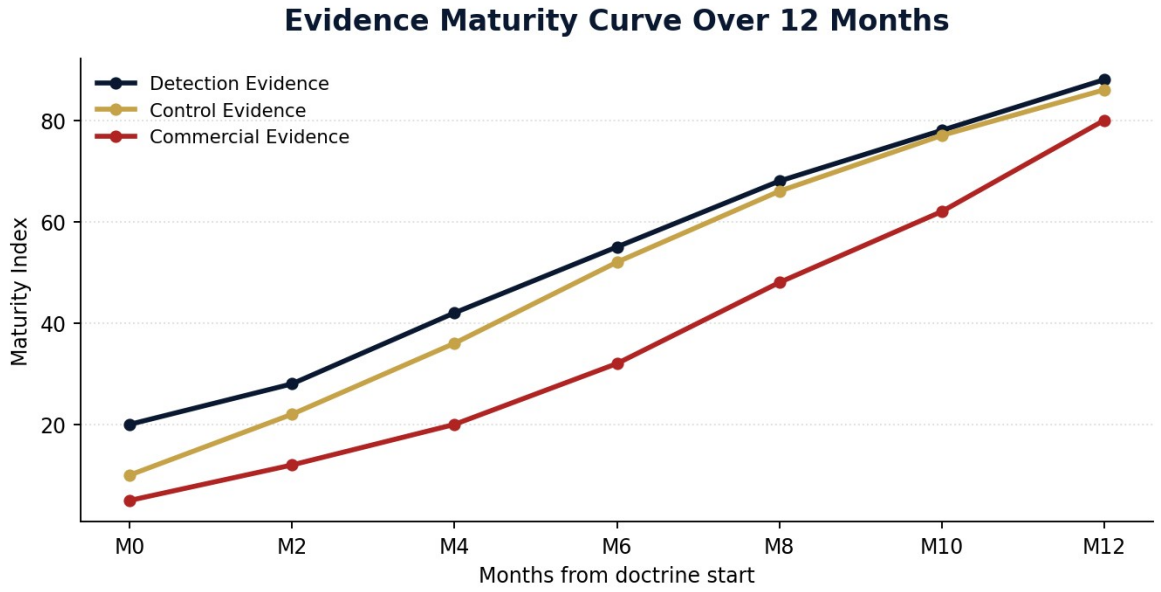


Figure 08-A. Evidence maturity does not arrive simultaneously — commercial evidence trails detection evidence by approximately four months in the median engagement.

09 REGULATORY CALIBRATION

DORA

DORA's resilience reporting is supported by attestable automation evidence.

NIS2

NIS2 notification windows are met more reliably when automation is audit-grade.

GDPR & Cross-Border Movement

GDPR Article 32 evidence is supported by attestable enforcement.

ISO 42001

ISO 42001 human-in-loop evidence is supported by audit-grade automation.

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 PLAYBOOK THAT THE REGULATOR SIGNED OFF

Sector: Tier-1 European Bank

Situation. A regulator audit required reconstruction of automated containment workflow for a candidate insider risk incident.

Intervention. Audit-grade automation doctrine had been operated for 11 months. Evidence was exported in 2 working days.

Outcome. Audit closed with positive commentary. Doctrine subsequently became the bank's reference for automation governance.

CASE STUDY • THE INSURANCE RENEWAL CALIBRATED BY EVIDENCE

Sector: Mid-Market Asset Manager

Situation. Cyber insurance renewal had been priced punitively due to opacity of automation governance.

Intervention. Doctrine engineered audit-grade evidence into the broker dossier.

Outcome. Renewal premium reduced by 14% on like-for-like cover. Broker reused the evidence as a benchmark for the carrier's regulated book.

11 BOARD REPORTING PLAYBOOK

Board reporting on audit-grade automation reports library health, attestation coverage, named-ownership currency, and commercial deployments.

Five Board Metrics That Move Decisions

Metric	What It Tells the Board	Doctrine Threshold
Attestation Coverage	Share of automated actions with attestation	100%
Named Owner Coverage	Share of playbooks with named owners	100%
Value Calibration Coverage	Share of playbooks with documented value definition	100%
Library Currency	Recency of last quarterly curation	≤ 90 days
Commercial Deployments	Reviews using automation evidence	Tracked

Companion Infographic — Board Governance Framework

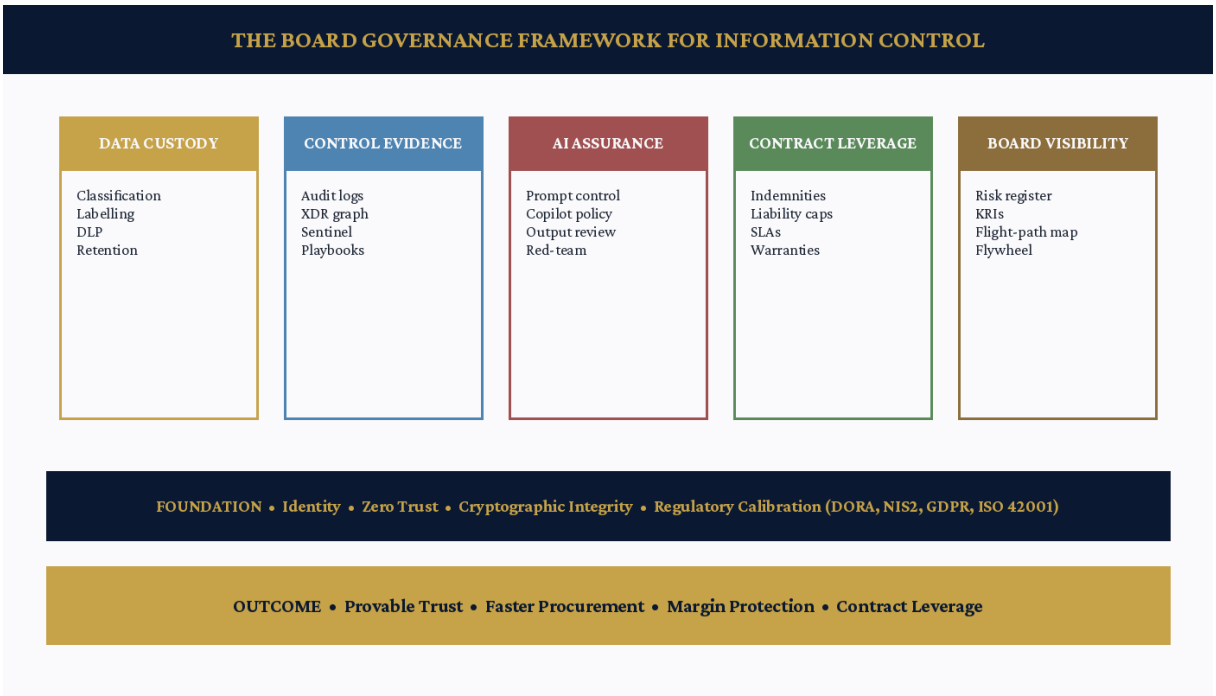


Figure 11-A. Five-pillar board governance framework for converting information control into commercial trust and contract leverage.

12 CONTRACT LEVERAGE & NEGOTIATION POWER

Audit-grade automation evidence is the differentiator that converts operational automation into commercial credential. The leverage compounds across procurement, regulator, and insurance interactions.

> *“Speed earns the deal once. Evidence earns it every time.”*
>
> — Doctrine

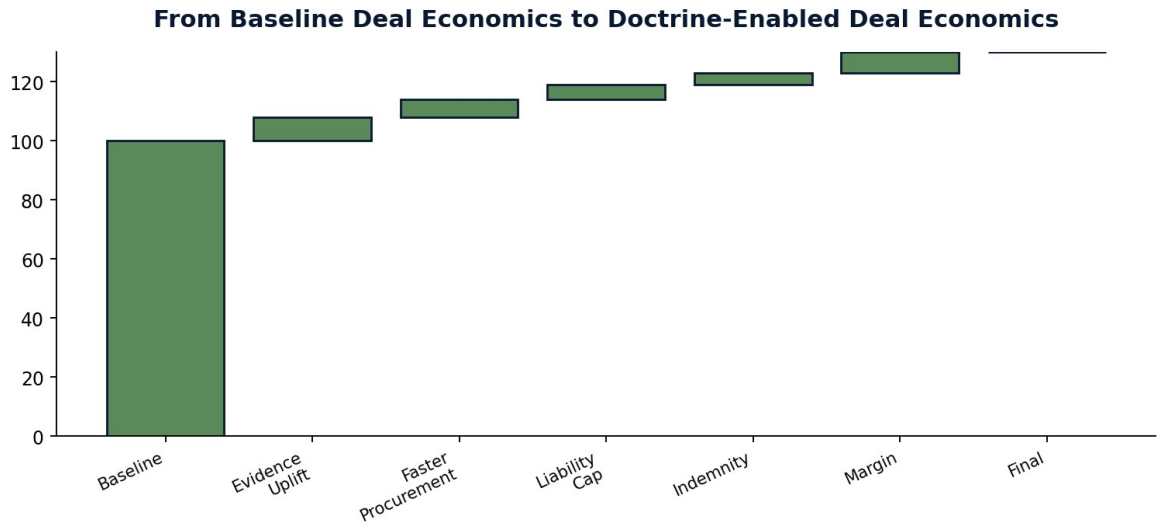
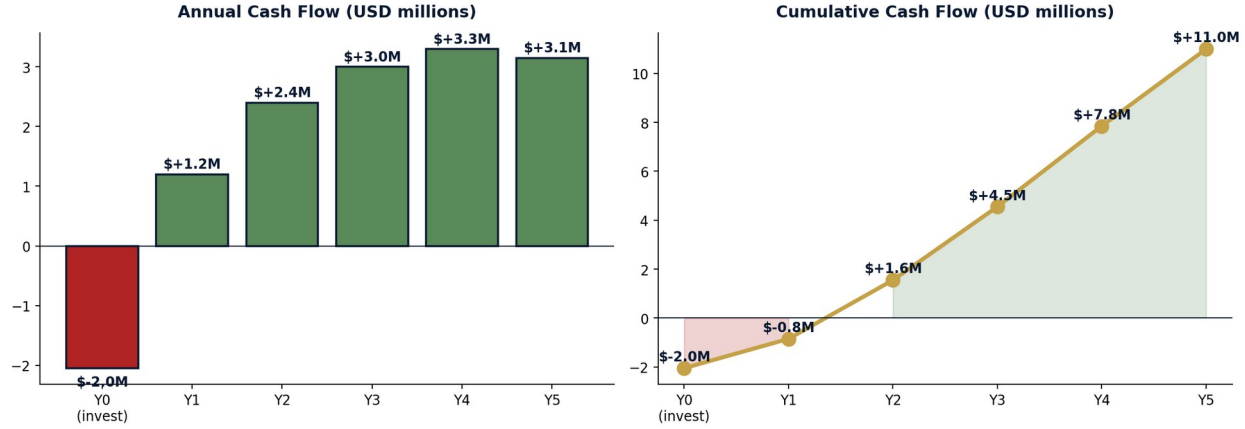


Figure 12-A. Cumulative deal-economics uplift attributable to commercially-weaponised control evidence.

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

This model quantifies the commercial return of operating the Automated Defence, Auditable Outcomes 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)	**$2.05M**
5-Year Cumulative Benefit	**$13.05M**
Net Present Value (10% discount)	**$7.49M**
Payback Period	**Year 2**
Internal Rate of Return (proxy)	**45%**
Benefit-to-Investment Ratio	**6.37×**

DOCTRINE ROI STATEMENT

The Automated Defence, Auditable Outcomes doctrine delivers $13.0M of cumulative benefit against $2.0M of investment over five years — a benefit-to-investment ratio of 6.4× 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 Automated Defence, Auditable Outcomes 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 Automated Defence, Auditable Outcomes 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 Automated Defence, Auditable Outcomes.

15 IMPLEMENTATION ROADMAP

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

Q1 • Attestation Substrate

- Engineer attestation into every playbook action
- Name owners for the existing playbook library
- Calibrate audit logging in Logic Apps
- Inventory current evidence gaps

Q2 • Workflow Reconstruction

- Engineer reconstructable workflow for SOAR sequences
- Audit playbooks against regulator-readability
- Calibrate value definitions per playbook
- Integrate evidence into the unified graph

Q3 • Library Curation

- Curate the playbook library
- Retire low-value or duplicative playbooks
- Engineer commercial export of automation evidence
- Pilot dossier against a procurement questionnaire

Q4 • Commercial Activation

- Apply doctrine in two strategic deals
- Defend a regulator or insurance review with automation evidence
- Brief the board on automation commercial attribution
- Establish quarterly curation cadence

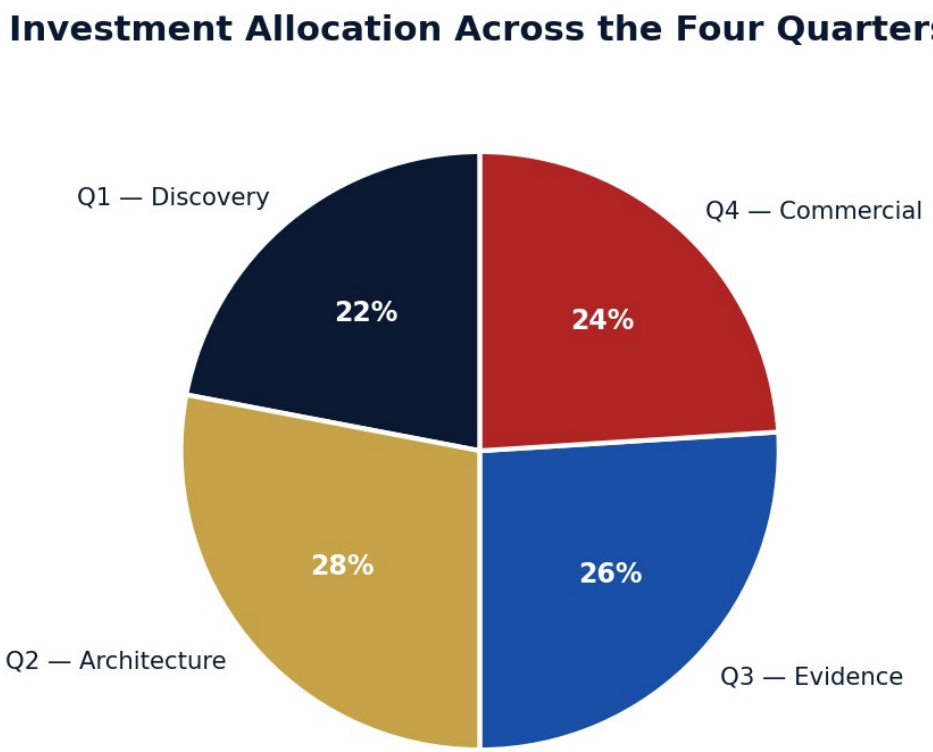


Figure 15-A. Balanced investment profile across the four-quarter implementation arc.

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 regulated enterprises operating Sentinel SOAR and Logic Apps automation in their security operations.

Total Addressable Market — Five-Year Projection

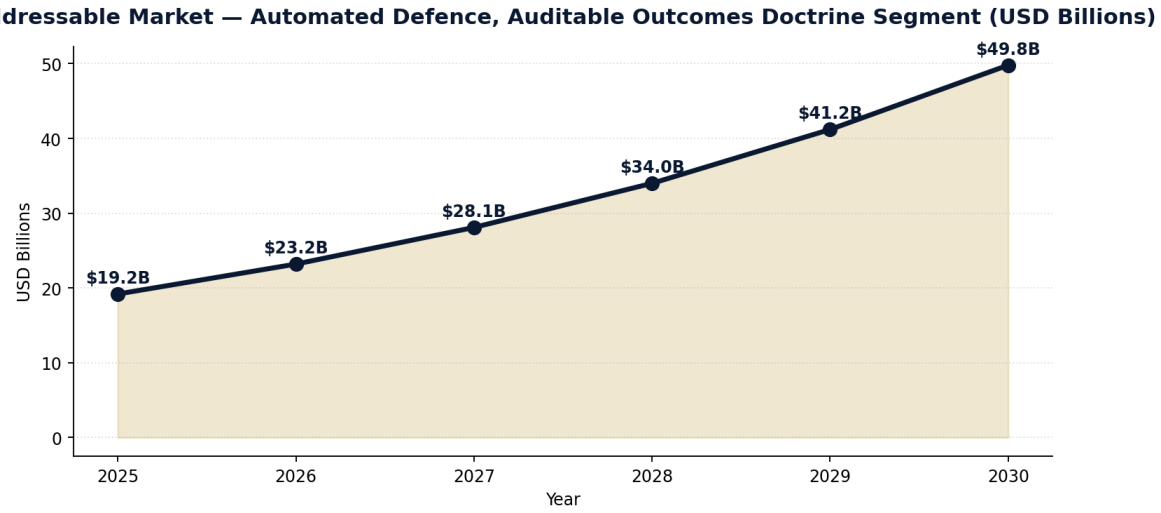


Figure MS-A. The doctrine-addressable market is projected to grow from approximately USD $19.2B (2025) to USD $49.8B (2030), representing a compound annual growth rate of 21%. Growth is structurally driven by regulatory expansion (DORA, NIS2, ISO 42001), AI-induced data governance demand, and the displacement of legacy point solutions by integrated doctrine.

FORWARD-LOOKING STATEMENT

The author projects that enterprises operating this doctrine to maturity will capture USD $9.0B in displaced procurement value by 2030 — equivalent to approximately 12% of the total addressable opportunity.

THE UPADRASTA AUTOMATED_DEFENCE INDEX™

The Upadrasta Automated_Defence 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.

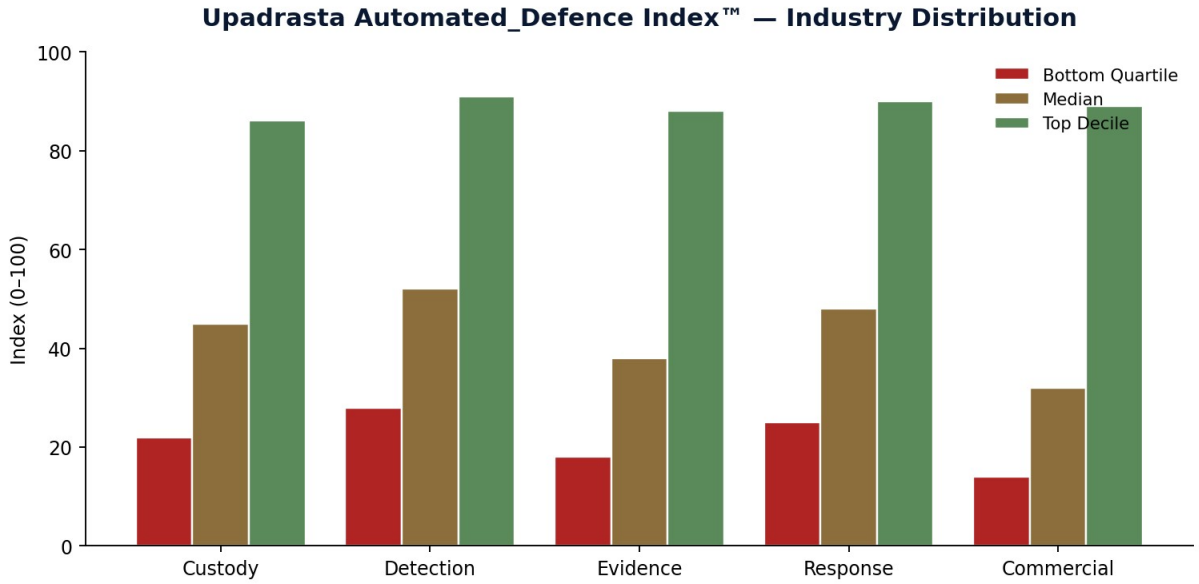


Figure PI-A. Distribution of Upadrasta Automated_Defence Index™ scores observed across regulated enterprise engagements. Top-decile enterprises score above 85 across all vectors; median enterprises score below 50; bottom-quartile enterprises score below 30.

INDEX DISCLOSURE

The Upadrasta Automated_Defence 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, every Sentinel playbook in regulated industries will require attestable evidence at the point of enforcement — with playbook audit becoming a standard internal audit programme.

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

Automation operated to audit grade is the doctrine that makes speed defensible. Without it, speed is risk. With it, speed is credential.

> *“Audit-grade automation is the only automation worth funding twice.”*
>
> — 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 Automated Defence, Auditable Outcomes.

60-Word Executive Quote

QUOTE — KIERAN UPADRASTA, SCHIPHOL UNIVERSITY

"Automation without evidence is speed without accountability. 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 Automated Defence, Auditable Outcomes 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

Automation without evidence is speed without accountability. 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 16. #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.

SIGNATURE DIAGRAM — PAPER 16

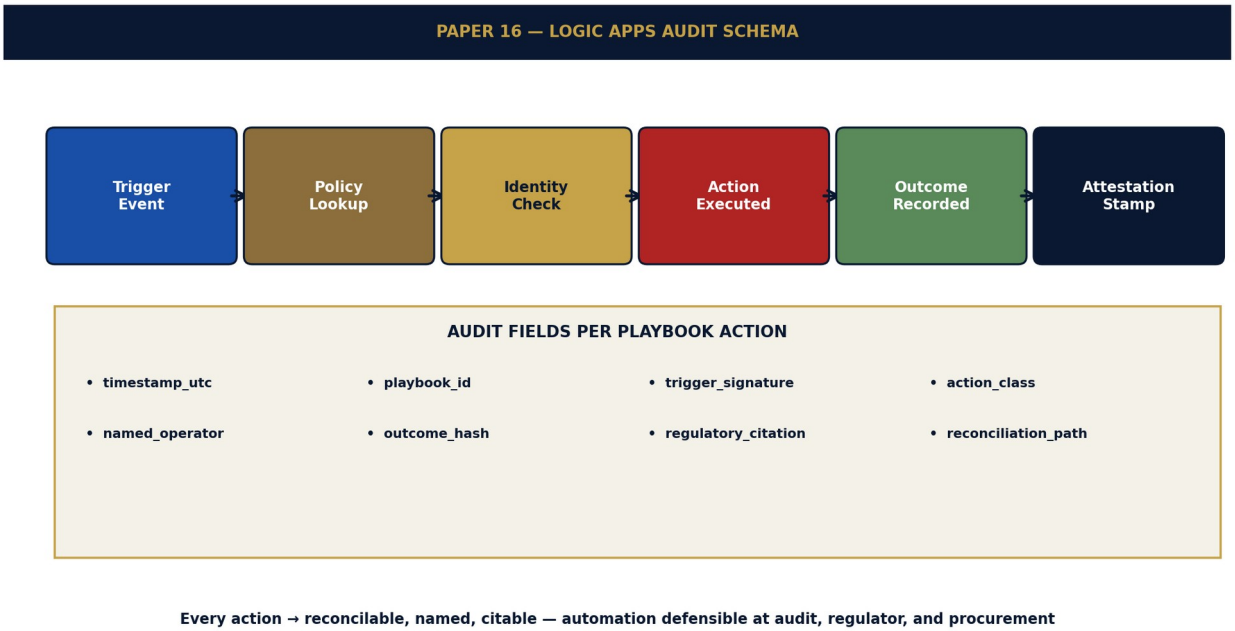


Figure SIG-16. Paper-unique signature diagram exclusive to the Automated Defence, Auditable Outcomes doctrine — engineered to be standalone-readable in procurement, regulator, and board contexts.

DEPLOYABLE TEMPLATE — PLAYBOOK ATTESTATION TEMPLATE

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
Field 1	Playbook Identifier	GUID + version stamp
Field 2	Trigger Signature	Hash of triggering rule + parameters
Field 3	Named Operator	Approver name or autonomous designation
Field 4	Action Class	Block / Isolate / Notify / Remediate
Field 5	Authorisation Basis	Policy reference + regulatory citation
Field 6	Execution Timestamp	ISO 8601 UTC
Field 7	Outcome Hash	Hash of final state + recovery evidence
Field 8	Audit Chain	Cryptographic chain to prior playbook execution

DEPLOYMENT STATEMENT
This template is the procurement-grade, board-deployable artefact specific to Paper 16. It is engineered to be lifted from this document and used in the regulated enterprise without re-keying or translation.

ATTRIBUTED BENCHMARK — AUDIT-GRADE AUTOMATION MATURITY DISTRIBUTION

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
Manual Only	12%	No automation; all containment manual
Partial Automation	31%	Automation without audit attestation
Automation + Logs	28%	Automation logged but not reconciled
Attestable Automation	21%	Named operator + timestamp + outcome hash
Audit-Grade Automation	8%	Reconcilable, regulator-readable, board-defensible

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 — BOARD-DEFENSIBLE PLAYBOOK TEMPLATE — SAMPLE AUDIT TRAIL

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
Trigger	Conditional Access risk spike + sign-in geo-velocity
Decision Rule	Auto-disable session if velocity > 1500 km/h
Owner	L1 SOC + auto-attestation
Action	Identity Revoke + Sign-Out enforced; user notified
Timestamp	ISO 8601 UTC + monotonic stamp
Evidence Log	Logic App execution ID + Sentinel SOAR audit record
Rollback	User restored on identity verification; auto-recorded
Regulatory Mapping	GDPR Art. 32; NIS2 incident-class evidence

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.