SOC20 Doctrine Series

Master Reference Card | v6.1 — Operational Artefacts (Polished)

Author: Kieran Upadrasta — MBA, BEng, CISSP, CISM, CRISC, CCSP. Professor of Practice — Schiphol University; Honorary Senior Lecturer — Imperials. 27 years cybersecurity; 21 years financial services; Big-4 (Deloitte, PwC, EY, KPMG) and Accenture. Contact: info@kieranupadrasta.com | www.kie.ie

Executive overview

The SOC20 Doctrine Series is a 20-paper, 837-page institutional doctrine for industrial security operations under DORA, NIS2, EU AI Act, and ISO 42001. The series translates operational telemetry into fiduciary state and converts cyber from a cost-line liability into a board-survivable, audit-defensible, and underwriter-recognised institutional posture.

This Master Reference Card is the navigator. A reader who needs to find the institution's Decision-Rights Architecture™ uses Section 5 below. A reviewer who needs to verify that the doctrine answers a specific regulatory or governance demand uses Section 7 (reviewer-ask map). A board member who needs the three-page reading list uses Section 6 (audience guide). The 837 pages are intentionally not summarised here; they are catalogued.

Series architecture

Every paper carries a uniform architecture so that any reader can navigate from any paper to its analogue in any other:

Section	Purpose
Cover + Précis + Authority	Author credentials; one-paragraph thesis; institutional standing
I. Thesis	The single proposition the paper defends
II. Failure Mode + II-bis Boundary + II-ter Formal Model	What is broken; the present-vs-target boundary; the mathematical model
III. Quantitative Evidence	Cohort-level numbers that anchor the thesis
IV. Architectural Doctrine + IV-bis Executable Artefact + IV-ter System Architecture	What to build; YAML/SQL/Python artefact; 3-lane diagram
V. Pareto + Cases + V-bis Worked Example	Where the institution focuses; numerical walk-through
VI. Board Mandate + VI-bis Market Positioning	What the board approves; cohort positioning quadrant
VII. 90-day Mandate	First-quarter execution plan; capital + owners + outcomes
VIII. Regulatory Anchors	DORA/NIS2/EU AI Act/ISO 42001/SEC mapping
IX. Evidence Chain + IX-bis Adversarial Review	What evidence proves it; what objections must be answered
X. Operating Model + X-bis Compounding Disciplines + X-ter Source Hierarchy	How it sustains; compounds; claim-by-claim source classification
X-quater Friction + X-quinquies Maturity + X-sexies Triage	Political/operational reality; L0–L5 ladder; Day-1 actions
X-septies Bonus (P01/05/07/14/17 only)	Paper-specific high-leverage block (P&L, boundary matrix, board pack, escrow cases, h
X-octies Close-Out Artefact	Paper-specific gap closure (anonymised case, ISAE template, OCSF migration, GDPR
X-novies Operational Artefacts	Paper-specific implementation deliverables (RACIs, governance matrices, lifecycle spec
XI. Strategic Outlook + XII. Closing Doctrine	Five-year hazard map; closing aphorism
Appendices A–F	Glossary, author/contact, methodology, citation map, bibliography, dataset disclosure

Per-paper artefact catalogue

Each of the 20 papers carries the architecture above; the catalogue below names the paper-specific artefacts that distinguish each paper from the next. Pages indicate where each artefact appears in the paper's PDF.

01	SOC Already Losing	Loss-accrual integral; piecewise λ_pre/λ_post	Decision-Rights Register YAML	Anonymised Tier-1 EU bank case (hour-by-hour T+0 to T+96); slope fit 3.69×	4-stage maturity roadmap + 6-KPI board scorecard
02	Alert Fatigue	Erlang-C M/M/c queueing model	Queue-depth SQL artefact	€4.7m capacity reallocation case; 9-month ρ trajectory	Rule suppression matrix (5 classes) + triage RACI
03	Detect ≠ Survive	Survival function S(t) with hazard rates	Order-of-restore YAML	Four-tier immutable backup architecture; recovery under AD destruction	T0/T1/T2/T3 register + 7-row order-of-restore + drill pass/fail
04	Pattern Drift	KL-divergence drift D_KL(P_t‖P_t-1) with Laplace smoothing	Pattern-drift monitor Python	Scattered Spider Q1→Q3 2024 distribution; D_KL=0.41; playbook retired	6-stage hypothesis lifecycle + playbook retirement register
05	Autonomous SOC	Closed-loop control: ζω_n settling-time bound	Closed-loop state-machine YAML	Full ISAE 3000 attestation template + auditor sign-off statement	Safety case + 4 misfire scenarios + regulator cross-examination
06	AI Arms Race	Two-player game with capital-allocation κ	Defensive AI Governance Pack	Anonymised 8-underwriter survey; premium cohort split –7% to +28%	AI control table + 4-regulator crosswalk + capital sensitivity
07	Boards Don't Understand	Translation function Φ from telemetry to fiduciary state	Three-page YAML board paper spec	Full 3-page board pack rendered (Decision/Evidence/Sign-off)	Legacy-vs-doctrine 8-dim comparison + RACI + Art. 5 challenge
08	Cost of Exposure	Exposure VaR_99 = quantile of Σ λ × Δ	Exposure VaR SQL	λ_pre derivation: 5-component breakdown (€62k/h per-incident)	VaR appetite workflow + data dictionary + board dashboard
09	Death of Manual IR	P(M < A): manual vs adversary loop time	Closed-loop containment Python	12-month cultural transition + 4-band comp realignment	11-action safety matrix + 5 failure modes

10	Noise Not Intelligence	Mutual information I(X;Y) yield score	Detection-truth scorer Python	OCSF migration: 4 phases + Splunk CIM→OCSF mapping; €1.75m–€3.75m cost	6-stage rule lifecycle + 7-control quality table + sample-size guidance
11	Drowning in Telemetry	Pareto frontier yield × volume; V* optimum	Telemetry rationalisation YAML	Top 5 noise sources named (CloudTrail, M365, EDR, NetFlow, DNS)	9-field Deletion Assurance Register + 3 non-repudiation controls
12	Future SOC	Operating-model elasticity: 4.2× engineering vs analyst	Headcount inversion plan YAML	6-role engineering cadre profile + comp bands €105k–€210k	Workforce transition plan + AI accountability + skills taxonomy
13	Compliance vs Resilience	Audit-survival gap $\Delta = \sigma_C - \sigma_R$; $e^{(\beta\Delta)}$ loss multiplier	Resilience attestation YAML	DORA 8-article mapping (Arts 5/6/9/11/17/24/28/30)	ISO 27001 Annex A crosswalk + paper-only retirement + continuity pack
14	Cyber as Revenue	Multiple Compression Index β_R, β_E with confidence bands	Cyber due-diligence pack	3 anonymised escrow cases (insurer/SaaS/industrial); –€34m, –€79.9m, –€84m	Sensitivity table + CFO/CISO/M&A RACI + 5-clause R&W library
15	Window of Exposure	Three-clock convolution; tail probability $P(T_W > t^*)$	Three-clock simulator Python	Out-of-band channel matrix (Teams/Signal/Bridge); drill scenario	Clock measurement standard + Three-Clock Board Pack + RACI + exception register
16	Yesterday's SOCs	Architectural debt growth $D(t) = D_0(1+r)^t$	Debt register YAML	18-month dual-run SIEM transition; 5 phases; rollback triggers	5-phase cutover playbook + 8-row legacy/target crosswalk + supervisor challenge
17	Detection Engineering	Coverage estimator $C = E[c(h)]$ with Wilson lower bound	Hypothesis register Python	Combinatorial set-cover ILP; greedy-vs-ILP empirical 4–9% uplift	10-field Detection Experiment Standard + confidence model + falsification appendix
18	IR Plan Will Fail	Wilson 95% lower bound on rolling drill pass-rate	Drill cadence YAML	Hostile drill safety guardrails (5 classes); 0 unplanned outages	8-scenario drill catalogue + 12-field evidence pack + 30-day remediation

19	Privacy Frontline	L_SR ↔ L_IR correlation ρ ≈ 0.71 [0.58,0.81]	Lineage register YAML	72-hour GDPR notification race timeline (T+0 to T+72)	7-role RACI + joint incident playbook + lineage R/A/G maturity
20	Winning AI Era	Compounding posture Π_t × (1+g)^T	Compounding simulator Python	Adopter-vs-deferrer cohort case; SVI +3.1 differential at T+4y	Series synthesis (P01–P19→5 chars) + Five-Quarter Programme + Board Paper template

Reviewer-ask → section mapping

Each row below records a specific reviewer demand (across four review rounds) and the section/page where it is answered. The mapping is reusable: it lifts directly into supervisor engagement, ISAE 3000 attestation scoping, and audit committee submission.

Maturity transition roadmap	P01	X-novies	4-stage roadmap (Conventional → Engineered → Autonomous → Board-Survivable)
Anonymised case walkthrough with slope fit	P01	X-octies	Tier-1 EU bank case; T+0 to T+96h; λ ratio 3.69×
Rule suppression governance matrix + FN control	P02	X-novies	5-class action matrix (suppress/tune/retire/escalate/retain)
Triage decision-rights RACI	P02	X-novies	9-decision RACI across L1/L2/Detection Eng/SOC Lead/CISO/Audit
Service-tier classification + order-of-restore register	P03	X-novies	T0/T1/T2/T3 + 7-row restore order + drill pass/fail criteria
Immutable backup engineering specifics	P03	X-octies	Four-tier architecture; key segregation; recovery time under AD destruction
Hypothesis-led detection lifecycle + playbook retirement	P04	X-novies	6-stage lifecycle + register + vendor-reach pack
Named threat-actor drift profile	P04	X-octies	Scattered Spider Q1→Q3 2024 distributions; D_KL=0.41
Closed-loop safety case + misfire appendix	P05	X-novies	Per-action preconditions + 4 misfires + regulator cross-examination
External assurance attestation template	P05	X-octies	ISAE 3000 Type 2 template + auditor sign-off statement
AI model-risk assurance + control crosswalk	P06	X-novies	5-control table + DORA/EU AI Act/ISO 42001/NIS2 crosswalk + scenario sensitivity
Anonymised underwriter survey data	P06	X-octies	8-underwriter premium cohort split
Legacy vs doctrine board-pack comparison	P07	X-novies	8-dimension comparison + RACI + Art. 5/Art. 20 challenge
Full three-page board pack specimen	P07	X-octies	Page 1 Decision / Page 2 Evidence / Page 3 Sign-off rendered
VaR risk-appetite calibration + data dictionary	P08	X-novies	6-step appetite workflow + 8-field dictionary + board dashboard
λ_pre derivation	P08	X-octies	5-component formula breakdown; €62k/h per-incident
Closed-loop containment safety matrix	P09	X-novies	11-action ranking observe → key destruction + 5 failure modes
Cultural transition framework	P09	X-octies	12-month plan; 4-band comp realignment; CISO 1:1 script
Detection rule lifecycle + signal-quality control + MI confidence	P10	X-novies	6-stage lifecycle + 7-control table + sample-size guidance
OCSF schema-sovereignty migration	P10	X-octies	4-phase migration; CIM→OCSF mapping; €1.75m–€3.75m cost
Deletion Assurance Register + non-repudiation + regulator challenge	P11	X-novies	9-field register + 3 non-repudiation controls + 5-Q challenge-response
Telemetry kill list (top 5 named)	P11	X-octies	CloudTrail / M365 admin / EDR low-conf / NetFlow east-west / DNS volume
Workforce transition + AI accountability + skills taxonomy	P12	X-novies	Quarterly transition + 10-decision matrix + 6-capability taxonomy
Engineering cadre profile (named roles + comp bands)	P12	X-octies	6 roles; €105k–€210k loaded; sourcing pattern; reskilling success

Audit-control to survival-test crosswalk	P13	X-novies	ISO 27001 Annex A crosswalk + paper-only retirement + board continuity pack
DORA article-by-article mapping	P13	X-octies	8 articles (5/6/9/11/17/24/28/30) — obligation/control/evidence/owner
Deal-sensitivity table + CFO/CISO/M&A RACI + R&W library	P14	X-novies	Posture/multiple sensitivity + operating model + 5-clause library
Practitioner peer-review acknowledgment	P14	X-octies	3 anonymised practitioners (M&A counsel, broker, PE diligence)
Clock measurement standard + Three-Clock Board Pack + exception register	P15	X-novies	Standard + single-page Board Pack + RACI + exception register
Out-of-band channel integration	P15	X-octies	Teams/Signal/Bridge matrix; drill scenario
Re-foundationing migration playbook + crosswalk + supervisor challenge	P16	X-novies	5-phase cutover + 8-row legacy/target crosswalk + challenge-response
Dual-run SIEM transition technical roadmap	P16	X-octies	18-month plan; rollback triggers; cost band
Detection Experiment Standard + coverage confidence + falsification	P17	X-novies	10-field standard + Wilson lower-bound model + top-10 falsification
Combinatorial optimisation framework	P17	X-octies	Set-cover ILP + Jaccard threshold + empirical 4–9% uplift
Drill catalogue + evidence pack + remediation workflow	P18	X-novies	8 scenarios + 12-field pack + 30-day remediation
Hostile drill safety guardrails	P18	X-octies	Blast-radius caps; 5-class pre-approval; abort triggers; SOP
Privacy-cyber RACI + joint incident playbook + lineage maturity	P19	X-novies	7-role RACI + T+0 to T+72 playbook + R/A/G maturity
72-hour GDPR notification race	P19	X-octies	Hour-by-hour timeline; lineage register usage per step
Series synthesis matrix + Five-Quarter Programme + Board Paper template	P20	X-novies	P01–P19 → 5-characteristic mapping + Q1–Q5 plan + 3-page template
Adopter vs deferrer cohort case	P20	X-octies	13-metric T+4 comparison; SVI +3.1 differential

Reading guide by audience

Different audiences read the series differently. The recommended reading orders below are calibrated to each audience's decision context.

Audit committee chair (3-paper read)	P07 (board translation) → P15 (three clocks) → P13 (compliance vs resilience). The chair leaves with: SVI as KPI, three-clock dashboard, compliance/resilience gap.
CISO (full read)	P01–P05 (operational doctrine) → P09–P12 (operating model) → P13 + P15 + P18 + P20 (governance). The CISO has the architecture, the operating model, the governance, and the capstone.
Group CRO (4-paper read)	P08 (Exposure VaR) → P14 (cyber as revenue) → P13 (resilience score) → P20 (compounding). The CRO sees the loss class, the deal impact, the resilience gap, and the trajectory.
Cyber underwriter (3-paper read)	P03 (recoverability evidence) → P05 (provable autonomy) → P14 (posture-conditional renewal). The underwriter has the institution's drill posture, autonomy posture, and renewal evidence pack.
Buy-side M&A diligence lead (2-paper read)	P14 (deal sensitivity + R&W library) → P16 (architectural debt). The diligence lead has the diligence pack format and the architectural risk model.
Supervisor / regulator analyst (3-paper read)	P05 (Article 14 oversight) → P13 (DORA mapping) → P18 (Article 11 testing). The supervisor has the autonomy oversight, the article-level mapping, and the drill posture.
Detection engineering lead (3-paper read)	P10 (signal yield) → P17 (hypothesis-led detection) → P04 (pattern drift). The lead has the yield framework, the hypothesis discipline, and the drift signal.
Academic citation / peer reviewer (full read recommended)	All 20 papers; Appendix F (methodology) on each. The series is anchored to a disclosed dataset (n=43; Q1 2023–Q1 2026); statistical methods are named per paper; bibliography is comprehensive.

Cross-cutting framework index

Eight proprietary frameworks recur across the series. The index below names where each framework is introduced and where it is operationally applied.

Board-Survivable Cyber Architecture™	P01	P05, P07, P09, P12, P20
Decision Rights Architecture™	P05	P01, P07, P09, P15, P18, P19
Evidence Chain Model™	P09	P01, P03, P05, P11, P13, P15, P18
Recoverability Mandate™	P03	P15, P18, P20
Contract Control Matrix™	P11	P10, P13, P14, P16
AI Accountability Stack™	P06	P05, P12, P19, P20
Survival Velocity Index™ (SVI)	P01	All papers (composite KPI)
Compounding-Institution Doctrine	P20	Synthesises P01–P19

Distribution and contact

The series is distributed under the author's institutional doctrine licence: audit-committee, regulatory-supervisor, academic, and underwriter use are authorised; redistribution and derivative work require written consent. The doctrine dataset (n=43, Q1 2023–Q1 2026) is held under non-disclosure with contributing institutions; reproducibility is bounded by Appendix F of each paper. For engagement, peer review, or institutional licensing: **info@kieranupadrasta.com | www.kie.ie**

If it cannot be evidenced, it cannot be defended.