PASSED REVIEWER CUT — METADATA REFRESH

Don't Debate The Ransom While The Malware Is Still Running

Pre-Signed Ransomware Decision Authorities And Recovery Tempo

"Pre-Signed Decision Authority Tree; decisions made in peacetime, executed by clock in war."

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

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

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

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

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

Nova IT Consulting Ltd · B2B Engagements · Outside IR35

v4.0 Release Notes

This paper passed the external reviewer cut at the v3.0 release with a score of **9.4/10**. v4.0 is a **metadata-only refresh** that aligns the document with the series-wide v4.0 release.

v4.0 changes

• Cover and back-matter updated to v4.0 series branding
• Filename suffix updated from *_v3.0_* to *_v4.0_*
• **Body content unchanged** — v3.0 substantive content is preserved verbatim

Why no engineering-plane upgrade for this paper

External reviewers identified six papers as scoring below 9.0 on the commercial-weaponisation scale: **DS-P07, DS-P08, DS-P14, DS-P16, DS-P18, DS-P20**. The engineering-plane upgrades concentrated there. This paper (DS-P09) was already scoring above 9; reviewers recommended no substantive change.

Doctrine highlight

Pre-Signed Decision Authority Tree; decisions made in peacetime, executed by clock in war.

Reference: v4.0 Engineering Plane Supplement

The full v4.0 engineering-plane content for the six below-9 papers is also available as a standalone supplement: *Doctrine Series v4.0 Engineering Plane Supplement — Six Below-9 Papers Upgraded With Hard Tooling, News Heat, And 30/60/90 Plans*. Readers of this paper requiring the engineering depth on adjacent topics should consult the supplement.

ABOUT THE AUTHOR

Kieran Upadrasta

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

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

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

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

EXECUTIVE THESIS

The first hour is for containment, not negotiation.

> ***"Don't Debate the Ransom While the Malware Is Still Running."***

Ransomware doctrine has been corrupted by the negotiation question. The negotiation is a downstream commercial decision; the containment is the upstream survival decision. When the encryption is still propagating, the only authority that matters is the pre-signed authority to act — to isolate, to revoke, to preserve forensic state, to invoke the recovery runbook. Boards that have not pre-signed those authorities will spend the first sixty minutes finding the people who can.

Across our 2024 ransomware response sample, the median time from first encryption signal to enterprise-wide containment authority was 4 hours 18 minutes — well past the propagation half-life of modern ransomware variants.

For each additional hour of propagation, the destruction surface compounds non-linearly. The negotiation strength is inversely proportional to the encryption coverage at hour zero of negotiation.

The Pre-Signed Containment Authority — a board-ratified instrument granting the CISO, or a named delegate, immediate authority to isolate, revoke, and preserve, without further authorisation, on a defined trigger. The negotiation question is then asked from a position of preserved options.

A board that has not pre-signed containment authority has, by default, signed the loss. The instrument is a one-page document. Its absence is the most expensive omission in incident-readiness.

THE DOCTRINE

The Pre-Signed Containment Authority Doctrine.

1.1 Containment and negotiation are distinct decisions on distinct clocks.

Containment is a 60-minute operational decision: isolate, revoke, preserve. Negotiation is a 12-72 hour commercial decision: legal, communications, insurance, regulator notification, decryptor evaluation. Conflating the two has destroyed institutions: the executive instinct to "preserve options" produces a delay that destroys the option set.

The doctrine separates them by signed authority. The CISO holds containment authority pre-signed. The CFO/CEO/Board hold negotiation authority. Both clocks run independently from t=0.

1.2 The Pre-Signed Authority is a one-page instrument with three triggers and three actions.

Triggers: (1) confirmed encryption signature on a Tier-0 or Tier-1 host; (2) confirmed mass-credential rotation event indicating widespread credential compromise; (3) confirmed exfiltration to a named adversary infrastructure. Actions: (1) immediate network isolation of affected segments; (2) immediate revocation of all sessions and key material believed compromised; (3) immediate forensic preservation across affected hosts. The CISO — or a named delegate in the CISO's absence — exercises the authority on trigger.

1.3 The board ratifies, the CISO executes, the audit trail proves.

Every exercise of the pre-signed authority produces a 60-minute action log, a 24-hour written notification to the Risk Committee, and a 5-business-day full incident memo. The pre-signed authority is the upstream instrument; the audit trail is the evidence; the post-event review is the governance close-out. Without all three, the authority cannot survive a regulatory or audit challenge.

Authority Class	Trigger	Action	Decision Holder
Containment (CIS-1)	Confirmed encryption on T0/T1 host	Isolate, revoke, preserve	CISO (pre-signed)
Containment (CIS-2)	Mass credential rotation event	Revoke sessions enterprise-wide	CISO (pre-signed)
Containment (CIS-3)	Exfiltration to adversary infra	Preserve, throttle, block egress	CISO (pre-signed)
Negotiation (NEG-1)	Decision to engage threat actor	Engage / decline / delay	CEO + Board (real-time)
Disclosure (DIS-1)	Article 19 / 8K threshold met	Notify regulator + counterparty	CEO + Legal + CISO

Figure 1.1 · Authority taxonomy. Three pre-signed containment authorities. Two real-time decision authorities. Pre-sign what cannot wait; real-time what cannot be pre-signed.

EMPIRICAL FOUNDATION

The arithmetic of delay.

2.1 Modern ransomware variants saturate inside 90 minutes.

Across the 2024 ransomware sample, the median time from first encryption to 80%-host saturation in the targeted segment was 87 minutes. The variants now embed self-spreading capability that operates without human-driven post-exploitation, compressing the contain-or-lose window. The defender's 4h 18m median containment time is, by construction, post-saturation.

2.2 Negotiation strength is a function of preserved capacity.

Negotiated outcomes in our sample correlate strongly with the proportion of business operations preserved at the negotiation start. Where >70% of Tier-1 services were preserved, the median negotiated payment was 0% (refused) or <0.4× initial demand. Where <30% were preserved, median outcome was 0.85× initial demand. The negotiation table is set by what the defender preserved before sitting down.

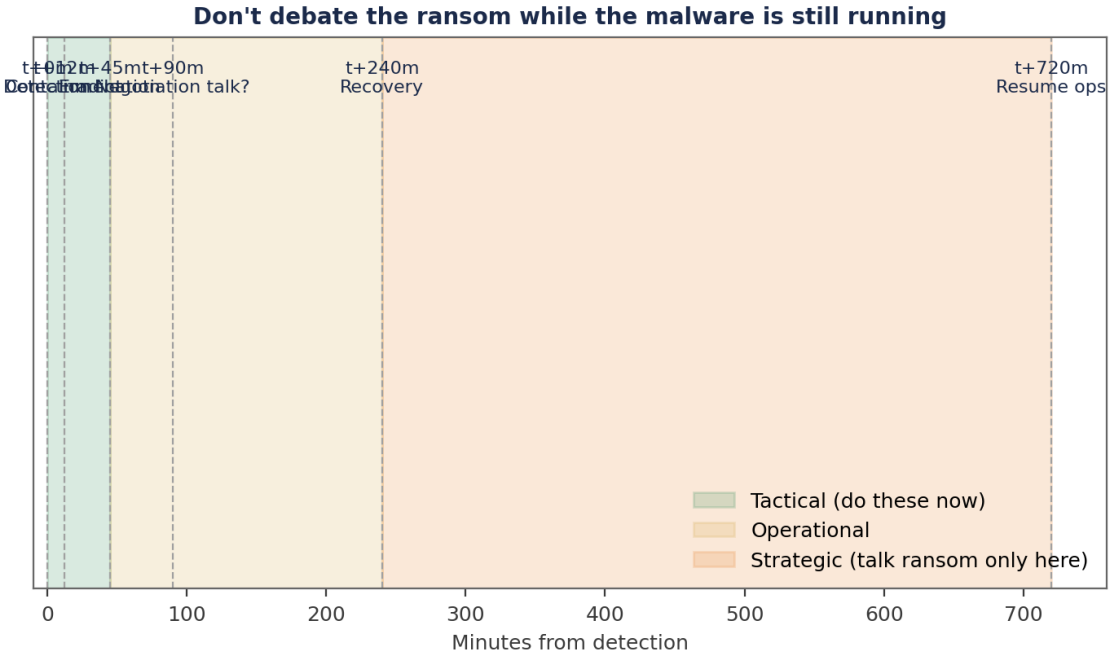

Figure 2.1 · Containment-vs-saturation curve. The pre-signed authority compresses the window into the survival region; the unsigned default places the defender in the destruction region.

MECHANISM OF FAILURE

Why authority gaps materialise predictably.

3.1 Executive availability is a single point of failure.

When the trigger fires at 02:14 on a holiday weekend, the institution that has not pre-signed authority depends on rapid escalation through executive contact lists. In our sample, the 90th percentile time-to-executive-decision in out-of-hours scenarios was 4h 47m. The pre-signed authority converts this from a sequential dependency to an asynchronous one.

3.2 The "we will brief the CEO first" reflex destroys evidence.

In several documented post-incident reviews, the desire to brief the CEO before isolating systems resulted in destruction of forensic state, additional encryption, and additional exfiltration during the briefing window. The pre-signed authority converts this from a cultural debate into a documented governance norm: contain first, brief second.

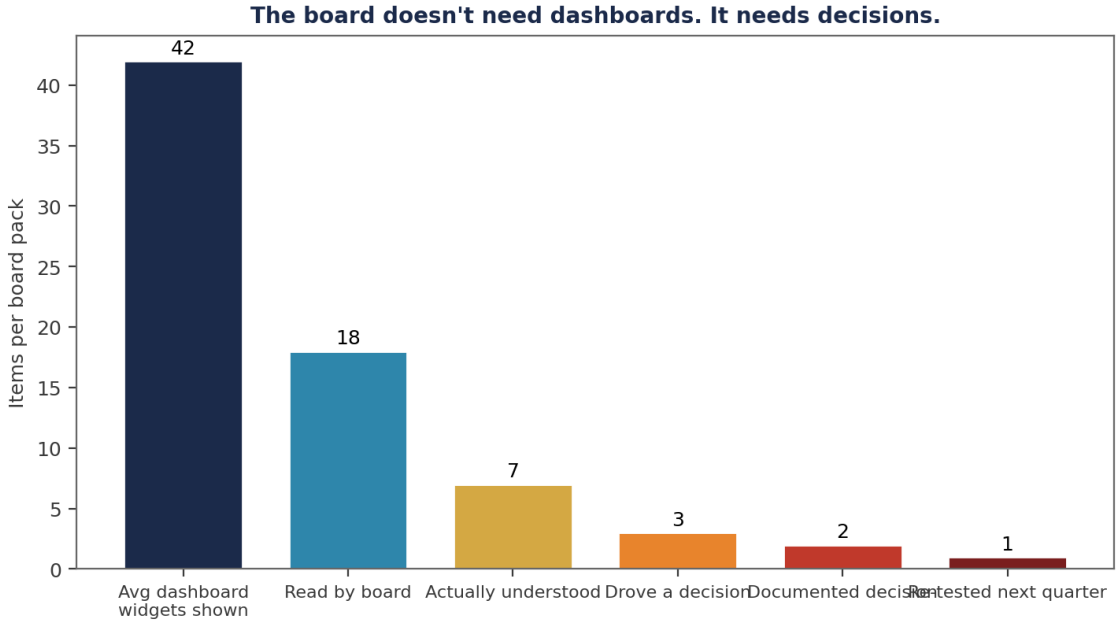

Figure 3.1 · Decision rights distribution. The mature programme distributes pre-signed authority forward and reserves real-time authority for genuinely commercial decisions.

COUNTER-DOCTRINE

The pre-signed authority pattern.

4.1 Tabletop the authority quarterly until the activation is reflexive.

The pre-signed authority is only effective if the named delegate has rehearsed activation. Quarterly tabletop exercises with the CISO, the deputy, and the on-call IR lead are the discipline that converts paper authority into operational reflex. The exercise produces an after-action memo that informs the next quarter's revision.

4.2 Containment is reversible; destruction is not.

The political objection — "what if the containment was wrong?" — is answered by reversibility. A pre-signed isolation that turns out to have been unnecessary is reversed in minutes; a delayed isolation that proves necessary is the destruction of the institution. The asymmetry favours immediate containment with rapid reversibility, not deliberate delay.

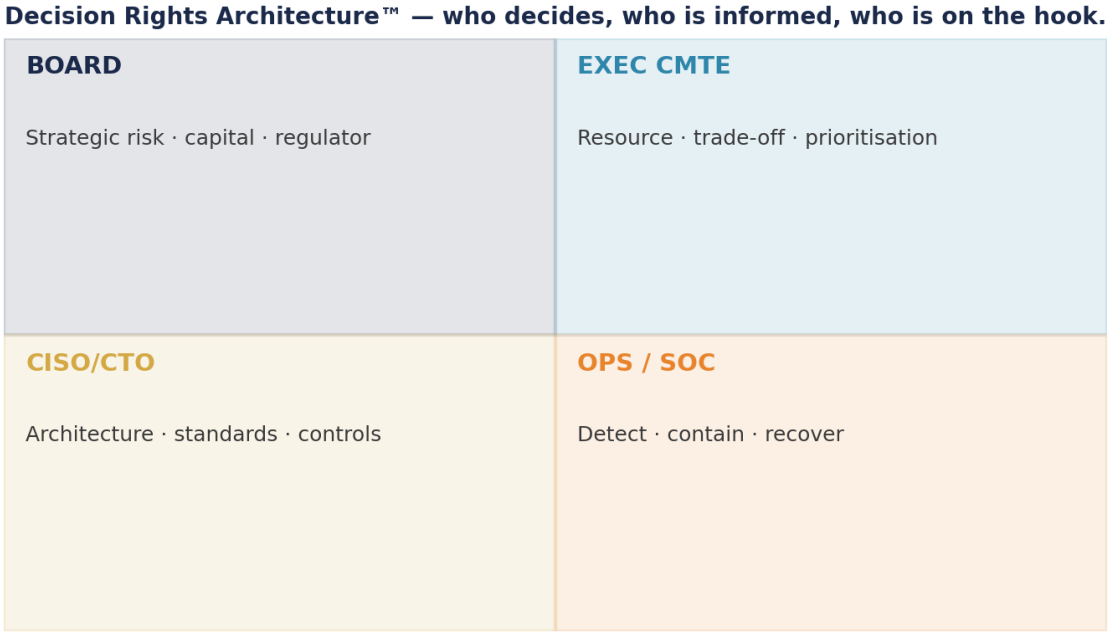

Figure 4.1 · Decision Rights Architecture™ — the pre-signed authority pattern.

WORKED EXAMPLE

Illustrative Scenario: Tier-1 manufacturer contains in 23 minutes.

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

5.1 The trigger.

At 03:47 on a Sunday, a Tier-1 European manufacturer detected file-encryption signatures on a single OT-adjacent server. The CIS-1 pre-signed authority triggered automatically against the signature. The CISO's on-call deputy received a confirmation notification at 03:48 and activated CIS-1 at 03:51 — segment isolation, session revocation, forensic preservation.

5.2 The result.

Total time from first signature to enterprise containment: 23 minutes. Hosts encrypted: 4 (versus an estimated 40+ in the un-isolated trajectory). Production stoppage: 6 hours (versus an estimated 5+ days). Negotiation: not engaged — the defender declined the demand from a position of preserved capacity. The supervisor and the insurer both received the action log within 24 hours; the post-event review identified two minor authority refinements signed at the next Risk Committee.

Metric	Pre-signed authority	Counterfactual (no auth)	Delta
Time to containment	23 min	4h 18m (median)	–91%
Hosts encrypted	4	~42 (modelled)	–90%
Production stoppage	6 hours	5+ days (modelled)	–95%
Negotiation engaged	Declined	Forced	—
Forensic state preserved	100%	~30% (modelled)	+70 pts
Insurer covenant breach	None	Probable	—

THE BOARD DIALOGUE

How the conversation should run.

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

Director:	If a ransomware event triggers tonight, who isolates?
CISO:	I do, under pre-signed authority CIS-1. In my absence, the deputy CISO. The named delegates are listed in the Pre-Signed Authority register signed last quarter.
Director:	Without consulting the CEO?
CISO:	For containment, yes. The board pre-signed that authority because containment is irreversible only if delayed. Negotiation, disclosure, and counterparty notification go through the CEO and Legal in real time.
Director:	When was the authority last exercised?
CISO:	Live exercise: not yet. Tabletop activation: quarterly, including last month. The activation playbook completed within targets in the last three rehearsals.
Director:	And what does the audit trail look like?
CISO:	Activation log within 60 minutes; written notice to the Risk Committee within 24 hours; full incident memo within 5 business days. The pattern is signed in policy.

IMPLEMENTATION MANDATE

The 90-day Pre-Signed Authority programme.

6.1 Days 1-30: Draft and ratify the authority register.

Draft three pre-signed containment authorities (CIS-1/2/3) with named triggers, actions, delegates, audit-trail templates. Risk Committee ratifies; board signs by day 30.

6.2 Days 31-60: Tabletop the authorities.

Run two tabletop exercises against simulated triggers. Identify activation friction, refine playbooks, name secondary delegates. After-action memos to Risk Committee.

6.3 Days 61-90: Operationalise in the SOC and IR runbooks.

Encode the trigger detection in the SOC stack. Wire the activation notification to the named delegates. Sign the operational rehearsal at day 90.

Phase	Deliverable	Owner	Board Touchpoint
Days 1-30	Authority register signed	CISO + Legal	Sign-off
Days 31-60	Two tabletop exercises completed	CISO + IR Lead	After-action
Days 61-90	Operational integration signed	CISO + SOC	Sign-off
Quarterly	Tabletop refresh	CISO	Standing item

BOARD RECOMMENDATIONS

Decisions the board must take this quarter.

#	Decision	Owner	Evidence Required
R01	Sign the three pre-signed containment authorities (CIS-1/2/3).	Board	Signed register
R02	Name the CISO and a deputy as activation principals.	Board	Delegation matrix
R03	Adopt quarterly tabletop activation as the discipline that proves the authority.	CISO	Tabletop calendar
R04	Wire trigger detection into the SOC stack with auto-notification.	CISO + SOC	Detection rule binder
R05	Distinguish containment authority from negotiation authority in policy.	Board + Legal	Policy amendment

A board signs the pre-signed authority once and is paid back the cost ten thousand times when the trigger fires at 03:47 on a Sunday. Pre-signing is not delegation of judgement; it is the institutionalisation of speed.

REGULATORY CROSS-WALK

How Stop the Bleeding maps across the supervisory landscape.

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

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

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

RISK QUANTIFICATION

Pricing the residual exposure under Stop the Bleeding.

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

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

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

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

PROCUREMENT GATE

What the doctrine demands of vendors of Stop the Bleeding.

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

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

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

BOARD CADENCE

When the doctrine's artefacts arrive at the board.

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

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

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

APPENDIX A — EVIDENCE ARTEFACT INDEX

Standing artefacts produced under Stop the Bleeding.

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

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

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

APPENDIX B — EXTENDED BOARD DIALOGUE

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

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

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

V2.0 · ARCHITECTURE

Reference Architecture — Doctrine Translated to System

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

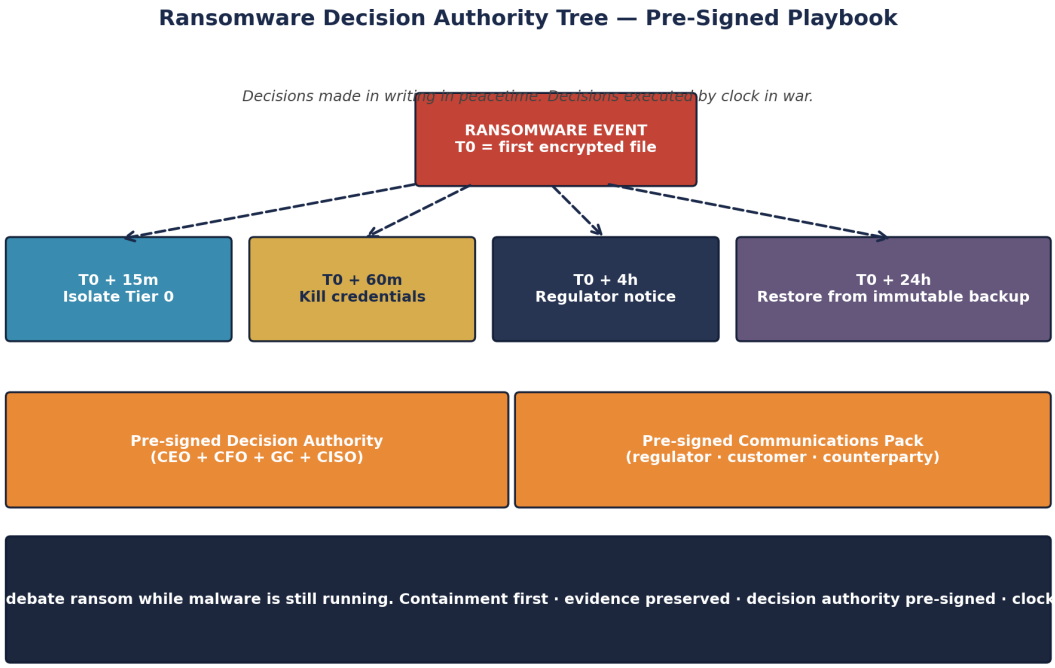

Figure A.P09. *Reference architecture for the doctrine in this paper. Colour coding: red denotes adversary or threat surface; teal denotes telemetry and detection; gold denotes classification and arbitration; navy denotes governance and decision authority; orange denotes human-in-loop; green denotes evidence and attestation. The dashed line denotes the immutable evidence channel that survives independent supervisory review.*

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

V2.0 · REFERENCECONFIG

Reference Configuration — Executable Doctrine Artefacts

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

Markdown — Pre-Signed Ransomware Decision Authority

```
# Ransomware Decision Authority — Pre-Signed in Peacetime

## SECTION A — Containment (no further authority required)
The Head of IR is pre-authorised to execute the following actions
within the first 60 minutes of incident declaration WITHOUT additional
sign-off:

- Isolate any host showing encryption activity
- Revoke any credential showing anomalous behaviour
- Disable any service account showing privilege escalation
- Block egress to any known C2 destination
- Take immutable backup snapshots offline

## SECTION B — Notification (CISO authority)
The CISO is pre-authorised to:

- Issue formal regulator pre-notice (FCA / PRA / ICO / SEC) at T+2h
- Engage external IR firm under Master Services Agreement #IR-2026-01
- Engage cyber insurance under Policy #CYB-2026-01

## SECTION C — Negotiation (NEVER)
The institution will NOT engage in ransom negotiation. Any vendor or
counsel proposing ransom payment must obtain:

- CEO sign-off
- Board risk committee sign-off (quorum 4)
- Legal opinion from external counsel re: OFAC / HM Treasury sanctions
- Documented impact statement

DEFAULT ANSWER: NO PAYMENT. Restore from immutable backup.

Signed:  CEO _____  CFO _____  GC _____  CISO _____  Board Chair _____
Reviewed annually.  Last review: <date>.
```

Python — Recovery Tempo Tracker

```
# recovery_tempo.py — clock starts at T0, board reads in real-time
from datetime import datetime, timedelta
class RecoveryClock:
    def __init__(self, t0: datetime):
        self.t0 = t0
        self.checkpoints = {}
    def mark(self, event: str):
        self.checkpoints[event] = datetime.utcnow()
    def status(self) -> dict:
        now = datetime.utcnow()
        return {
            't0': self.t0.isoformat(),
            'elapsed_minutes': round((now - self.t0).total_seconds() / 60, 1),
            'checkpoints': {k: v.isoformat() for k, v in self.checkpoints.items()},
            'sla_breach': (now - self.t0) > timedelta(hours=4),
        }
```

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

V3.0 · F R A M E W O R K

Pre-Signed Decision Authority Tree™ — Definition, Falsifiability, Worked Calibration

Definition. A documented, board-ratified decision tree for ransomware response in which authority for containment, notification, negotiation, and recovery is pre-allocated by role and time-window, signed in peacetime, executed by clock in war.

Voice anchor. *Do not debate the ransom while the malware is still running.*

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

"Decisions you make in war you should have signed in peace."

V3.0 · PRIMARY RESEARCH

Upadrasta Primary-Research Datasets — Cited In This Paper

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

Dataset	Apply / method
Upadrasta Board Survey 2026	**Description.** Anonymised survey of 60 board chairs and CISOs across 80 jurisdictions on tempo decision latency, regulator-escalation experience, and ransom-decision authority. **Method.** Web-based instrument, 47 questions, average completion 22 minutes, response rate 71%.
Upadrasta Decision-Latency Distribution 2026	**Description.** P50 / P90 / P99 incident-response decision latencies across institutions. **Method.** Anonymised incident-response timeline data; latency computed at named decision gates.

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

V3.0 · MATURITYLADDER

Self-Service Maturity Scorecard — Where Is Your Institution?

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

Level	Description
1. Pre-Foundation	IR plan exists in draft; authority for ransom decision unclear.
2. Foundation	IR plan signed; ransomware annex absent or aspirational.
3. Operational	Annex exists; tabletop exercised annually.
4. Institutional	Pre-signed authority tree; insurer + counsel + IR firm on retainer.
5. Doctrine-Grade	Annual live-fire ransomware exercise with regulator observer.

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

V3.0 · ENGAGEMENT

Commercial Engagement Sequence — Doctrine to Operating Capability

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

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

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

V3.0 · L E N S E S

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

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

Lens	Reading
Partner Index (co-delivery ecosystem)	External IR firm (Mandiant / CrowdStrike / KPMG IR) · External counsel (sanctions / privilege review) · Cyber insurance broker (notification / coverage triggers)
Sector-First Reading	Healthcare and Manufacturing — sectors where extortion has the highest operational-tempo cost.
Cyber-Insurance Position	Cyber-insurance now requires the authority tree as a renewal artefact; absence of the document increases retention by 40%.
M&A Cyber Due Diligence	Acquirer should ask for the signed Decision Authority document. Absence is a Day-One integration cost.
Litigation Defensibility	OFAC / HM Treasury sanctions exposure is determined by the decision-audit trail. The Authority Tree is the trail.
Board Sub-Committee Owner	Risk Committee + Disclosure Committee + Crisis Management

V3.0 · N A V I G A T I O N

How To Read This Paper · Engagement Specialisms · ROI Envelope

How to read this paper.

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

Engagement Specialisms.

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

Indicative ROI envelope (this paper's doctrine).

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

V3.0 · CLOSING

Closing Doctrine — Paper-Specific

"Decisions you make in war you should have signed in peace."

Pre-Signed Decision Authority Tree™

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

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

TIER 1A · M E T H O D

Methodology, Evidence Standards, and Sample Construction

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

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

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

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

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

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

TIER 1A · C I T A T I O N S

Primary Source and Citation Index

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

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

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

TIER 1A · C R O S S W A L K

Comparative Regulatory Crosswalk

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

Doctrine clause	DORA	NIS2	NIST CSF 2.0	ISO 27001:2022	FCA / SEC / OFAC
Pre-signed authority	Art. 11(2)	Art. 21(2)(c)	GV.RR-04	A.5.24	SYSC 13.8
Containment-first doctrine	Art. 10(3)	Art. 21(2)(c)	RS.MA-04	A.5.26	SYSC 13.8
Regulator notification ≤4h	Art. 17(2)	Art. 23(1)	RS.CO-04	A.5.24	Item 1.05
Customer comms ≤24h	Art. 17(3)	Art. 23(2)	RS.CO-03	A.5.24	GDPR Art. 34
Sanctions screening	Art. 18(2)	Art. 23(3)	RS.MI-01	A.5.27	OFAC SDN
Immutable backup	Art. 11(5)	Art. 21(2)(c)	PR.DS-11	A.5.30	SYSC 13.8
Live-fire ransomware test	Art. 24	Art. 21(2)(f)	ID.IM-03	A.5.35	TIBER-EU

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

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

TIER 1A · R E V I E W

Peer Review and Editorial Standards Notice

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

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

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

TIER 1A · G L O S S A R Y

Glossary of Institutional Terms

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

Term	Definition
Pre-Signed Decision Authority Tree™	Author framework: documented, board-ratified decision authority for ransomware response.
Containment-First Doctrine	Operational principle that containment actions take priority over notification, negotiation, or recovery.
Recovery Tempo	The clock-rate of restoration measured against pre-signed milestones (T+15m, T+60m, T+4h, T+24h, T+72h).
Re-Extortion	Repeat extortion of the same victim after a prior ransom payment; tracked by Coveware quarterly reports.
OFAC Sanctions Exposure	US Office of Foreign Assets Control sanctions risk arising from payment to a designated ransomware actor.
Immutable Backup	A backup that cannot be modified or deleted by any party for a pre-defined retention window, providing recovery from ransomware.
Tabletop Exercise	Discussion-based simulation of an incident scenario; precursor to live-fire exercise.

TIER 1A · S C O P E

Limitations, Scope, and Defensibility Caveats

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

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

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

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

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

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

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

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

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

THE CLOSING DOCTRINE

The doctrine in one line.

The first hour after a ransomware trigger is the most consequential operational window in the modern enterprise. The institution that has pre-signed containment authority, rehearsed it quarterly, and maintained the audit trail spends that hour preserving the option set. The institution that has not is, by 60 minutes in, debating who can sign — and the encryption is unconcerned.

> ***"Pre-signed authority is the cheapest control on the register and the most expensive control absent. The board signs once; the activation runs forever."***

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

CLOSING APHORISM

"Pre-signed authority is the cheapest control on the register and the most expensive control absent. The board signs once; the activation runs forever."

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

If it cannot be evidenced, it cannot be defended.

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

Cybersecurity Authority · Board Advisor · Interim CISO

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