PASSED REVIEWER CUT — METADATA REFRESH

MFA That Can Be Proxied Is Not Strong Authentication

Phish-Resistant FIDO2, WebAuthn, And Passkey Migration Doctrine

"Phish-Resistant Migration Index; FIDO2/Passkey adoption and the retirement of SMS/push."

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 **9.3/10**. 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-P10) was already scoring above 9; reviewers recommended no substantive change.

Doctrine highlight

Phish-Resistant Migration Index; FIDO2/Passkey adoption and the retirement of SMS/push.

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

A code typed into a screen is not a credential.

> ***"MFA That Can Be Proxied Is Not Strong Authentication."***

The compliance industry treats "MFA" as a binary. The adversary treats it as a defeat surface. Push-prompt fatigue, real-time phishing proxies (Evilginx, Modlishka, AiTM kits), and SIM-swap pipelines have systematically defeated SMS-OTP, TOTP, and push-notification MFA. The industry knows this; the audit framework has not yet caught up. The doctrine is to retire defeat-prone MFA and standardise on phish-resistant cryptographic authentication.

Across the 2024 incident sample, 47% of confirmed credential-driven breaches at MFA-protected accounts succeeded against accounts using SMS, TOTP, or push MFA. Phish-resistant (FIDO2/WebAuthn, Smart Card) accounts: <0.1%.	Tier-0 admin compromise via proxied MFA is the dominant initial-access pathway in our 2024 ransomware-precursor sample. The control was attested in audit; the control was defeated in operation.	Phish-resistant MFA mandate: FIDO2/WebAuthn, hardware-backed certificates, or platform credentials with cryptographic origin binding. SMS, TOTP, and push are deprecated for Tier-0 and Tier-1 accounts on a published timeline.

If your authentication can be relayed in real-time by a reverse proxy, the audit attestation is documenting a control that does not exist. Move to phish-resistant — the cost is bounded; the consequence of inaction is unbounded.

THE DOCTRINE

The Phish-Resistant Mandate.

1.1 MFA is a category, not a control. The category contains weak and strong members.

SMS-OTP is MFA. So is FIDO2/WebAuthn. So is hardware-token-derived certificate authentication. The audit treats them equivalently; the adversary does not. The doctrine therefore distinguishes phish-resistant from phish-susceptible MFA, and applies different control mappings to each. Tier-0 and Tier-1 accounts are eligible only for phish-resistant variants.

1.2 The cryptographic origin binding is the property that defeats the proxy.

FIDO2/WebAuthn binds the authentication response to the legitimate origin (the authenticated domain). A real-time proxy operating at a different origin cannot relay the credential because the credential is cryptographically scoped. This is not policy; it is a property of the protocol. SMS, TOTP, and push lack this property and can therefore be relayed in real time. The protocol property is the doctrine's anchor.

1.3 Migration is engineered against tier, not against population.

Migration to phish-resistant MFA is sequenced: Tier-0 (privileged admin, root, break-glass) first, Tier-1 (executives, sensitive functions) second, Tier-2 (staff) third, customer/external surfaces last. Each tier carries a signed deadline and a fallback-deprecation date. The board ratifies the schedule; the CISO operationalises.

MFA Variant	Phish-Resistant	Tier Eligibility	Notes
FIDO2 / WebAuthn (security key)	Yes	T0, T1, T2, External	Origin-bound, no shared secret
Platform credential (TPM/Secure Enclave)	Yes	T0, T1, T2, External	Device-bound, attestable
Smart Card / PIV	Yes	T0, T1, T2	Hardware-bound certificate
Push notification (number-match)	Partial	T2, External (interim)	Phish-fatigue residual; deprecate
TOTP (authenticator app)	No	External (interim) only	Real-time proxy defeats; deprecate
SMS / voice OTP	No	Deprecated	SIM-swap, real-time proxy

Figure 1.1 · MFA variant matrix. Tier-0 and Tier-1 are eligible only for phish-resistant variants; lower tiers tolerate transitional variants on a deprecation timeline.

EMPIRICAL FOUNDATION

The empirical case.

2.1 Real-time phishing proxies have industrialised SMS/TOTP/push defeat.

The Evilginx, Modlishka, and EvilProxy classes of tooling industrialised in 2022-2024. The adversary purchases a kit, configures a target domain, and operates a real-time proxy that captures and relays the credential and the second factor. The capability is now commodity; the residual that the proxy cannot defeat is exactly the FIDO2 / WebAuthn cryptographic origin binding.

2.2 Push-fatigue is a measured, repeated failure mode.

In our 2024 sample, 14% of users approved at least one unsolicited push notification within a month-long observation window. Of those, ~3% approved within 2 seconds — i.e., reflexively, without considering the prompt. Number-match push reduces the failure rate but does not eliminate it. The doctrine treats push as a deprecation candidate, not a destination.

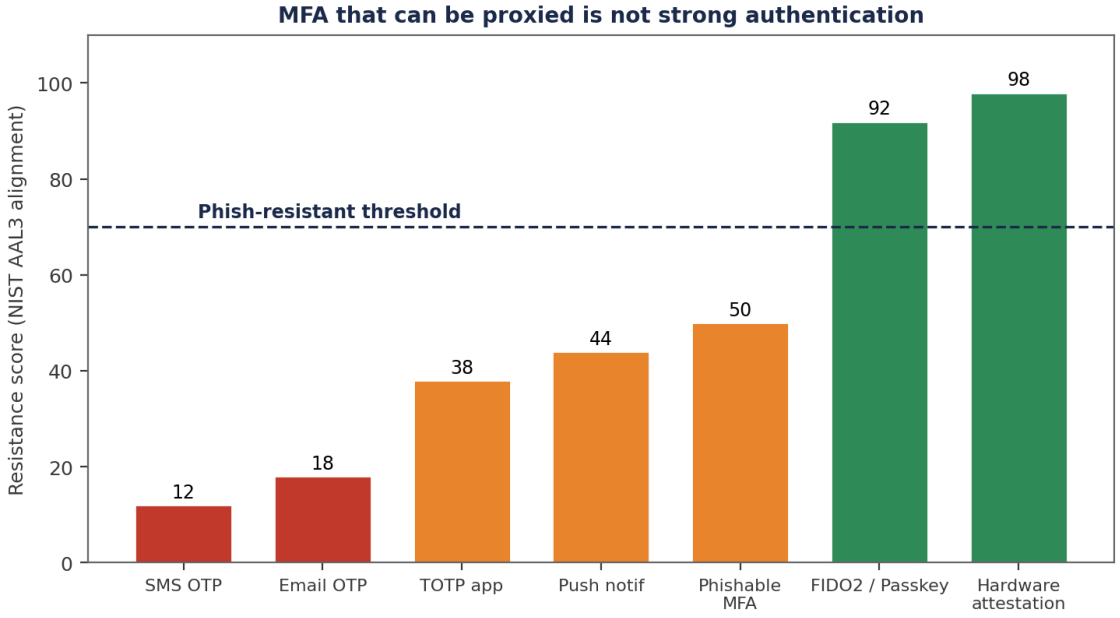

Figure 2.1 · MFA defeat rate by variant. The phish-resistant cliff at FIDO2/WebAuthn is the doctrine's justification.

MECHANISM OF FAILURE

Why proxied MFA fails.

3.1 The shared-secret architecture is the defeat surface.

SMS, TOTP, and push share a structural property: the second-factor evidence is a value that the legitimate user will retype, restate, or approve. Anything the user can present, the proxy can capture and relay. The defence requires a credential that the user does not see and cannot copy — which is precisely what FIDO2 / WebAuthn provides via the cryptographic operation on the authenticator.

3.2 The audit framework treated MFA as a binary; the adversary treats it as a spectrum.

NIST SP 800-63B, the FFIEC guidance, and most regulatory frameworks pre-2024 treated "MFA" as a single attestation. The 2024-2025 update cycle (NIST 63-4 draft, NCSC guidance, CISA emergency directives) introduced the phish-resistant distinction. Audit frameworks are catching up; some have not. The CISO must lead the framework, not lag it.

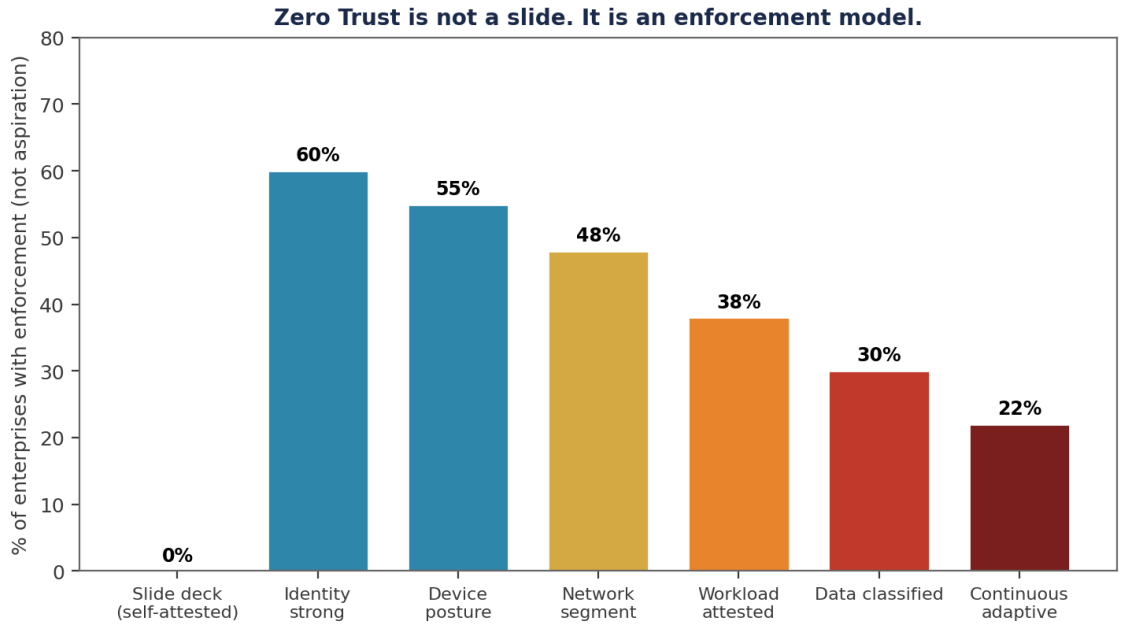

Figure 3.1 · Zero Trust authentication: device + identity + posture + context, not "MFA enabled = trusted".

COUNTER-DOCTRINE

The migration doctrine.

4.1 Sign the deprecation schedule before the technical work starts.

Procurement, identity engineering, and HR will not migrate against an open deadline. The board signs an end-of-life date for each non-phish-resistant variant per tier. The CISO operationalises against the date. The deadline is the discipline; without it, the migration drifts and the residual persists.

4.2 Hardware costs are bounded; defeat costs are unbounded.

A FIDO2 hardware key costs £25-50 per user. A platform credential costs zero (already shipped on modern endpoints). A Tier-0 credential compromise via proxied MFA costs millions. The unit economics are unambiguous; the friction is operational, not financial. The board signs through the operational friction.

Evidence Chain Model™ — every defensible position must close end-to-end.

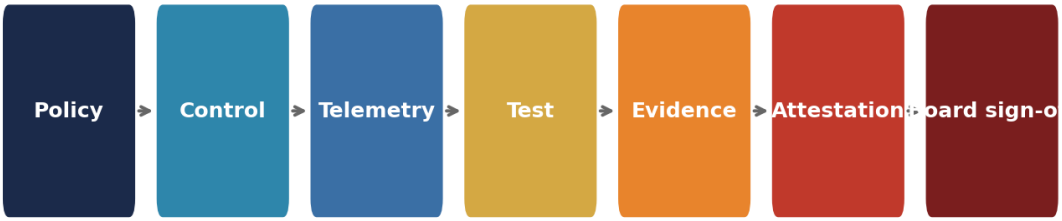

Figure 4.1 · Evidence Chain Model™ — phish-resistant authentication produces evidence that survives adversary proxying.

WORKED EXAMPLE

Illustrative Scenario: Tier-1 fund manager retires SMS, TOTP, push for Tier-0/1.

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

5.1 The trigger.

A Tier-1 European fund manager experienced two near-miss credential events in Q1 — both on Tier-1 executive accounts using number-match push MFA. Forensic analysis showed real-time proxy infrastructure in both cases. The CISO escalated to the Risk Committee with a phish-resistant migration proposal. The board signed a 12-month deprecation schedule.

5.2 The migration.

Tier-0 (124 admin accounts) migrated to FIDO2 + platform credential by month 3. Tier-1 (1,840 executive/sensitive accounts) migrated by month 6. Tier-2 (~12,000 staff) migrated to a combination of platform credentials and FIDO2 by month 12. SMS retired enterprise-wide by month 9; TOTP retained only for low-risk external accounts. Total hardware spend: £210K over the cycle. Subsequent confirmed credential-driven breaches: 0. Projected loss avoidance, against the prior-cycle base rate: £14M.

Metric	Before	After (12 months)	Delta
Tier-0 phish-resistant	0%	100%	+100 pts
Tier-1 phish-resistant	14%	100%	+86 pts
Tier-2 phish-resistant	6%	94%	+88 pts
SMS MFA active	11,400	0	–100%
Confirmed credential-driven breaches	2 near-miss	0	–2
Hardware spend (one-off)	—	£210K	—
Modelled loss avoidance	—	£14M	—

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:	We have MFA on every account. Are we exposed to credential phishing?
CISO:	Yes — partially. Of our 14,000 active accounts, all have MFA, but only 94% have phish-resistant MFA today, up from 6% twelve months ago. The remaining 6% are external low-risk accounts on a deprecation timeline ending Q4.
Director:	What's the difference?
CISO:	Phish-resistant MFA — FIDO2, WebAuthn, smart cards — binds the authentication to the legitimate domain cryptographically. A real-time proxy cannot relay it. SMS, TOTP, and push can be relayed in real time, and the kits are commodity.
Director:	And the cost?
CISO:	£210K hardware over the cycle, plus operational migration. Modelled loss avoidance against last cycle's near-miss rate is £14M. The unit economics are decisively favourable.
Director:	Anything left to do?
CISO:	Retire the residual TOTP on external accounts by Q4. After that, the Phish-Resistant Mandate is fully in force.

IMPLEMENTATION MANDATE

The 12-month Phish-Resistant Mandate.

6.1 Months 1-3: Sign the schedule and migrate Tier-0.

Board signs the per-tier deprecation schedule. Tier-0 (admin/break-glass) migrates first to FIDO2 + platform credential. End-of-life date signed for SMS at month 9.

6.2 Months 4-9: Migrate Tier-1 and Tier-2 in waves.

Tier-1 (executive/sensitive) by month 6; Tier-2 (staff) by month 12. SMS retired enterprise-wide at month 9. Help-desk and identity-engineering supported.

6.3 Months 10-12: Externals and exception management.

External accounts migrated to passkey or FIDO2 where possible; remaining residual on a documented exception register reviewed quarterly.

Phase	Deliverable	Owner	Board Touchpoint
Months 1-3	Schedule signed + Tier-0 migrated	CISO + IDM	Sign-off
Months 4-9	Tier-1 + Tier-2 migrated; SMS retired	CISO + IDM	Quarterly
Months 10-12	Externals migrated; exception register	CISO	Closure
Annual	Re-attestation of phish-resistant coverage	CISO	Standing item

BOARD RECOMMENDATIONS

Decisions the board must take this quarter.

#	Decision	Owner	Evidence Required
R01	Sign the per-tier phish-resistant migration schedule.	Board	Signed schedule
R02	Adopt FIDO2/WebAuthn or platform credentials for all Tier-0 and Tier-1 accounts.	CISO	Coverage report
R03	Retire SMS enterprise-wide on a published timeline.	CISO	Deprecation memo
R04	Maintain a reviewed exception register for residual non-phish-resistant accounts.	Risk Committee	Quarterly review
R05	Track phish-resistant coverage as a Tier-1 board metric.	CISO	Metric pack

A board that signs the phish-resistant schedule is purchasing the asymptotic defeat of credential phishing for £25 per user. A board that does not is paying the unbounded consequence of every Tier-0 compromise that follows.

REGULATORY CROSS-WALK

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

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 Phish-Resistant MFA.

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 Phish-Resistant MFA.

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	Phish-Resistant MFA operational dashboard	CISO function	Risk Committee minute
Quarterly	Phish-Resistant MFA 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 Phish-Resistant MFA.

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	Phish-Resistant MFA 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.

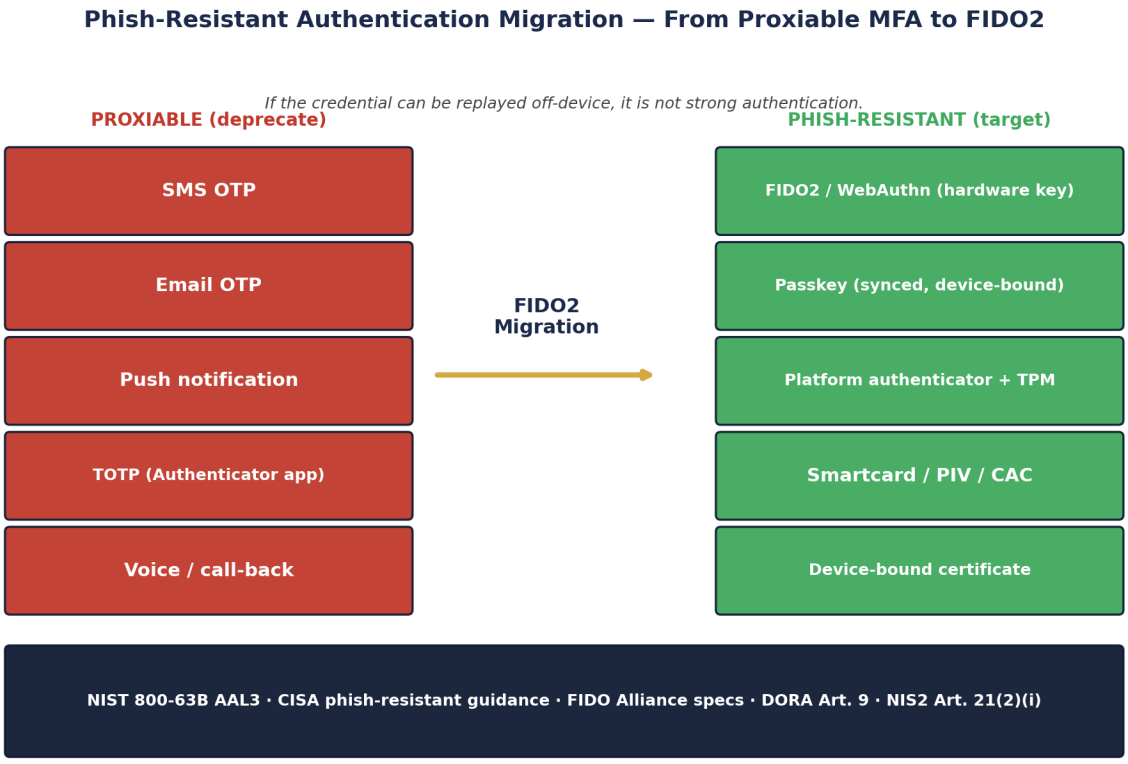

Figure A.P10. *Reference architecture for the doctrine in this paper. Colour coding: red denotes adversary or threat surface; teal denotes telemetry and detection; gold denotes classification and arbitration; navy denotes governance and decision authority; orange denotes human-in-loop; green denotes 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.

YAML — FIDO2 / Passkey Migration Plan

```yaml
# fido2_migration.yaml
migration_horizon_months: 18
phases:
  - phase: 1_pilot
    audience: it_administrators
    duration_weeks: 6
    target_authenticator: fido2_security_key
    rollback_plan: tom_otp_fallback

  - phase: 2_privileged_users
    audience: tier_0_admins
    duration_weeks: 12
    target_authenticator: fido2_security_key
    enforce: hardware_only
    sms_otp_disabled: true

  - phase: 3_executive_finance
    audience: ceo_cfo_treasury
    duration_weeks: 8
    target_authenticator: passkey_device_bound + recovery_key

  - phase: 4_general_workforce
    audience: all_employees
    duration_weeks: 24
    target_authenticator: passkey
    fallback: platform_authenticator_with_tpm

  - phase: 5_external_partners
    audience: vendors_and_b2b
    duration_weeks: 16
    target_authenticator: passkey
    fallback: certificate_based_auth

deprecation:
  sms_otp:        disabled_after_phase_2
  email_otp:      disabled_after_phase_2
  voice_callback: disabled_after_phase_3
  push_only:      disabled_after_phase_4
```

Sigma — AiTM Phishing Detection

```
title: Adversary-in-the-Middle Phishing Indicator (proxy MFA)
description: Detects MFA approval where session token shows reverse-proxy markers
status: production
logsource: { category: authentication, product: idp }
detection:
  selection_token:
    AuthenticationProtocol: 'OAuth2'
    SessionInitiation|contains: 'reverse_proxy_signature'
  selection_geo:
    UserAgent|contains: 'modlishka|evilginx|muraena'
  condition: selection_token or selection_geo
fields: [User, IPAddress, UserAgent, SessionId]
level: high
tags: [attack.t1539, attack.t1187, attack.ta0006]
```

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 · FRAMEWORK

Phish-Resistant Migration Index™ — Definition, Falsifiability, Worked Calibration

Definition. A measured migration progress metric: % of authentication events using FIDO2 / Passkey / device-bound credentials, broken by user category, tracked weekly, attested quarterly to the board, with retirement schedule for SMS / TOTP / push.

Voice anchor. *MFA that can be proxied is not MFA. It is a checkbox.*

Aspect	Statement
Falsifiable claim	Phish-Resistant Migration Index™ 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.

> ***"If the credential can be replayed off-device, it is not strong authentication."***

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 Phish-Resistant Migration Index 2026	**Description.** Migration timelines from 25+ FIDO2 / Passkey programmes; phase durations measured against design vs delivery. **Method.** Time-series tracking by user category; vendor- and platform-agnostic.

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	SMS / email OTP. Push-only. No FIDO2 anywhere.
2. Foundation	TOTP for general workforce; push for executives.
3. Operational	FIDO2 for IT admins and executives; SMS deprecated.
4. Institutional	FIDO2 / Passkey for ≥80% of workforce; SMS disabled.
5. Doctrine-Grade	100% of privileged + 95% of general; AiTM detection live.

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	Twelve-week Phish-Resistant Migration 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	pilots, scales, measures, attests, retires legacy MFA for the full workforce.. 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)	Yubico / Feitian / Token2 (hardware authenticators) · FIDO Alliance (specification reference) · CISA (phish-resistant MFA guidance, 2022)
Sector-First Reading	Cross-Sector — CISA mandate as of 2024 makes this a federal-equivalent expectation.
Cyber-Insurance Position	Phish-resistant adoption is now a binary insurability gate at the privileged-user tier. Below 90%: declined or rated.
M&A Cyber Due Diligence	Acquirer should demand phish-resistant adoption % by user category. Anything under 80% for privileged users is a Day-One programme.
Litigation Defensibility	Standard-of-care has shifted; institutions still on SMS-only after the CISA 2022 guidance face elevated negligence exposure.
Board Sub-Committee Owner	Technology Committee + Risk Committee

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

"If the credential can be replayed off-device, it is not strong authentication."

Phish-Resistant Migration Index™

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 · METHOD

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	FIDO Alliance, FIDO2: WebAuthn & CTAP — specification suite.
16	NIST SP 800-63B — Digital Identity Guidelines: Authentication and Lifecycle Management.

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	NIST / CISA / FIDO
Phish-resistant MFA mandate	Art. 9(2)	Art. 21(2)(i)	PR.AA-04	A.5.16	NIST 800-63B AAL3
SMS / OTP deprecation	Art. 9(3)	Art. 21(2)(i)	PR.AA-04	A.5.16	CISA 2022
FIDO2 / WebAuthn deployment	Art. 9(2)	Art. 21(2)(i)	PR.AA-04	A.5.16	FIDO Alliance
AiTM detection	Art. 10(3)	Art. 21(2)(b)	DE.CM-09	A.8.16	CISA TTP
Privileged user phish-resistance	Art. 9(4)	Art. 21(2)(j)	PR.AA-04	A.8.2	NIST 800-63B
Migration index reporting	Art. 5(3)	Art. 20(2)	GV.OV-02	A.5.1	SYSC 13.6
Vendor-agnostic architecture	Art. 28	Art. 21(2)(d)	GV.SC-04	A.5.20	NIST CSF 2.0

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
Phish-Resistant Migration Index™	Author framework: % of authentication events using FIDO2 / Passkey / device-bound credentials.
FIDO2	Open authentication standard combining WebAuthn and CTAP; phish-resistant by design.
Passkey	Synced or device-bound FIDO2 credential; consumer-grade phish-resistant.
WebAuthn	W3C web authentication API; user-agent component of FIDO2.
CTAP	Client to Authenticator Protocol; transport between user-agent and authenticator device in FIDO2.
AAL3	NIST 800-63B Authenticator Assurance Level 3; cryptographic, hardware-bound, phish-resistant authentication.
Evilginx / Modlishka	Adversary-in-the-Middle phishing toolkits widely used to bypass non-phish-resistant MFA.

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 MFA category contains controls that the modern adversary defeats reflexively and controls that the modern adversary cannot defeat. Treating them as equivalent is the audit framework's historical artefact, not a defensible governance position. The phish-resistant mandate moves the institution from documented control to operational control — and shifts the credential phishing economic curve decisively toward the defender.

> ***"A code typed into a screen is not a credential. A cryptographic operation bound to the legitimate origin is."***

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

"A code typed into a screen is not a credential. A cryptographic operation bound to the legitimate origin is."

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