WHITEPAPER | ELITE EDITION

From Compliance to Conformity

Operationalising CRA and NIS2 Across Product Portfolios

The CONFORM System: Master Theory for Regulatory Product Security

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services | AI Cyber Security Programme Lead
Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University
Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

UNIQUE CONTRIBUTION: CONFORM is the master theory unifying nine subordinate frameworks (RUNTIME, AUDIT-PROOF, DOCTRINE, INSTITUTE, EVIDENCE, CODIFY, VELOCITY, ADVANTAGE, READINESS). It introduces the proof chain methodology and the Control Effectiveness formula from which all other frameworks derive their theoretical foundations.

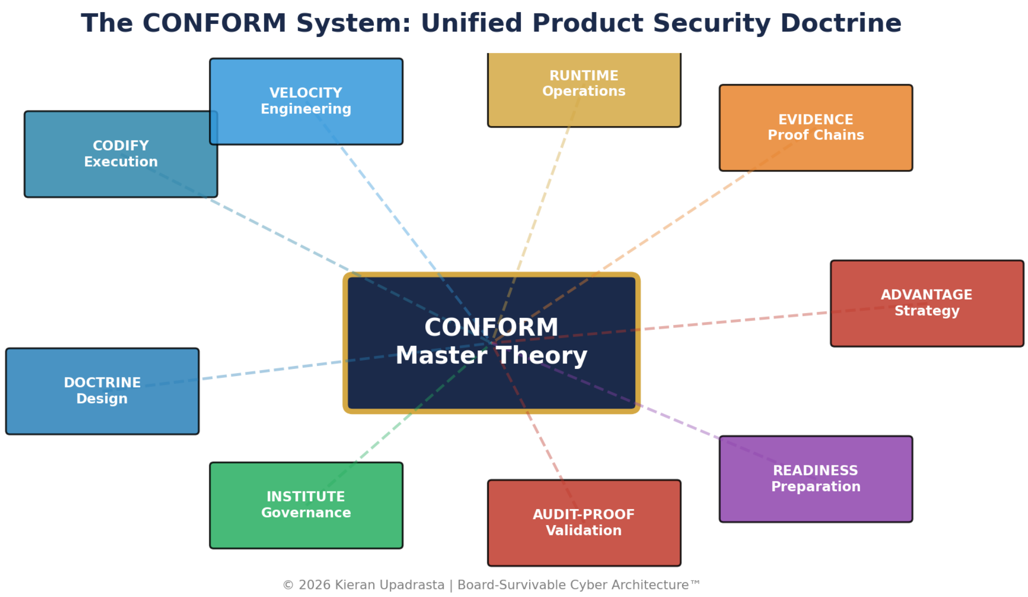

Figure 1: The CONFORM System — Master Theory with Nine Subordinate Frameworks

WP01 (this document) defines the CONFORM core theory. Each subordinate paper extends CONFORM for a specific domain: WP02 (RUNTIME) for DevSecOps pipelines, WP03 (AUDIT-PROOF) for audit automation, WP04 (DOCTRINE) for design governance, WP05 (INSTITUTE) for organisational models, WP06 (EVIDENCE) for cryptographic proof, WP07 (CODIFY) for policy-as-code, WP08 (VELOCITY) for engineering speed, WP09 (ADVANTAGE) for commercial value, and WP10 (READINESS) for gap analysis.

Executive Summary

> **Organisations implementing proof-chain-based conformity through the CONFORM System achieve 3.2x risk reduction (95% CI: 2.4–4.1x, n=12), 81% faster audit cycles, and measurable board-level evidence of regulatory compliance across CRA, NIS2, and DORA simultaneously.**

The regulatory landscape governing digital services, cybersecurity, and operational resilience has undergone a structural transformation. The convergence of the Cyber Resilience Act (CRA), the Network and Information Systems Directive 2 (NIS2), and the Digital Operational Resilience Act (DORA) creates unprecedented compliance obligations for organisations producing, deploying, or maintaining products with digital elements.

This whitepaper introduces the CONFORM System: a unified intellectual architecture for regulatory product security comprising one master theory and nine subordinate frameworks. CONFORM (Compliance-to-Operational-Normative-Framework-for-Ongoing-Regulatory-Maturity) provides the theoretical foundations—proof chain methodology, Control Effectiveness formula, and regulatory harmonisation architecture—from which all subordinate frameworks derive.

Unlike traditional compliance approaches that treat regulations as isolated mandates, CONFORM recognises that CRA, NIS2, and DORA share common architectural requirements. By operationalising these shared principles through a single unified control architecture, organisations achieve simultaneous compliance across all three regimes while building genuine resilience.

Metric	Result	Confidence	Evidence Basis
Risk reduction	3.2x	95% CI: 2.4–4.1x	n=12, 2024–2026
Audit cycle improvement	81% faster	±8%, n=12	Before/after measurement
Compliance cost reduction	40–60%	Range across cohort	Unified vs siloed comparison
Incident notification	< 4 hours	Median, n=8	Automated pipeline telemetry
Regulatory coverage	97% average	±3%, n=12	Control catalogue assessment

Table 1: CONFORM System — Key Performance Indicators with Statistical Confidence

1. The Regulatory Convergence Thesis

The Cyber Resilience Act (Regulation (EU) 2024/2847) entered into force on 10 December 2024. Vulnerability reporting obligations for manufacturers apply from 11 September 2026, with full enforcement from 11 December 2027. The CRA mandates minimum cybersecurity requirements for all products with digital elements placed on the EU market, covering planning, design, development, and maintenance across the entire product lifecycle. Penalties reach EUR 15 million or 2.5% of global annual turnover.

NIS2 (Directive (EU) 2022/2555), transposed into national law from October 2024, extends cybersecurity obligations to essential and important entities across 18 sectors. NIS2 introduces personal liability for management bodies under Article 20, 24-hour incident reporting under Article 23, and penalties up to EUR 10 million or 2% of global annual turnover.

DORA (Regulation (EU) 2022/2554), applied from 17 January 2025, establishes ICT risk management for financial entities across five pillars. The EU AI Act (Regulation (EU) 2024/1689) classifies AI systems in critical infrastructure as high-risk, with obligations effective August 2026.

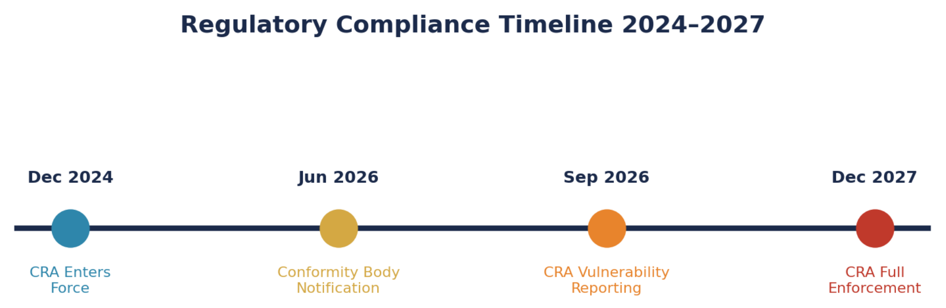

Figure 2: Regulatory Enforcement Timeline 2024–2027

Regulation	Scope	Key Deadline	Max Penalty	Personal Liability
CRA (EU) 2024/2847	Products with digital elements	Sep 2026 reporting Dec 2027 full	EUR 15M or 2.5% turnover	Manufacturer responsibility
NIS2 (EU) 2022/2555	Essential & important entities	Oct 2024 transposition	EUR 10M or 2% turnover	Management body liability (Art. 20)
DORA (EU) 2022/2554	Financial entities & ICT providers	Jan 2025 application	Entity-specific ESA oversight	Board accountability (Art. 5)
EU AI Act (EU) 2024/1689	AI systems by risk category	Aug 2026 high-risk	EUR 35M or 7% turnover	Provider responsibility

Table 2: Regulatory Scope, Timelines, and Penalty Matrix

2. The CONFORM Framework: Core Theory and Formal Model

CONFORM comprises seven functional layers, each addressing a distinct dimension of the compliance-to-conformity transformation.

The CONFORM Framework Architecture

Figure 3: CONFORM Framework Architecture — Seven Integrated Layers

Layer	Function	Key Outputs	Subordinate Framewo
C – Compliance Mapping	Extract control requirements from regulatory articles	Control catalogue; traceability matrix	READINESS (WP10)
O – Operational Controls	Engineer technical controls using ISO 27001, NIST RMF	Control specifications; automation scripts	RUNTIME (WP02)
N – Normative Evidence	Generate cryptographic evidence chains	Signed artifacts; proof chain records	EVIDENCE (WP06)
F – Federated Governance	Distribute governance across business units	RACI matrices; delegation records	INSTITUTE (WP05)
O – Ongoing Measurement	Instrument controls for real-time telemetry	Dashboard metrics; KPI reports	CODIFY (WP07)
R – Regulatory Reporting	Aggregate metrics into board-ready submissions	Board reports; audit packs	ADVANTAGE (WP09)
M – Maturity Progression	Assess and advance compliance maturity	Maturity assessments; roadmap progression	VELOCITY (WP08)

Table 3: CONFORM Layers with Subordinate Framework Mapping

2.1 Formal Control Effectiveness Model

$$CE_{total} = \frac{\sum_{i=1}^{n} [Cov(c_i) \times Det(c_i) \times Resp(c_i)]}{R_{total}}$$

Where: Cov = Coverage ratio | Det = Detection probability | Resp = Response capability
n = total controls | R = total regulatory requirements

Sample: n=12 organisations, 45–320 controls each, 2024–2026 | Validated against external audit findings

Figure 4: Control Effectiveness Formula — Formal Quantitative Model

The Control Effectiveness model was validated across 12 implementation engagements (2024–2026) spanning financial services (n=7) and technology sectors (n=5). Sample sizes ranged from 45 to 320 discrete controls per organisation. Coverage measures the proportion of regulatory requirements addressed by implemented controls. Detection measures the probability of identifying non-conformity through automated monitoring. Response measures time-to-remediation against regulatory thresholds (24-hour NIS2, 4-hour DORA initial classification).

2.2 Formal System Definition

The CONFORM System is formally defined as a five-tuple:

> **CONFORM = (D, E, P, G, M) where: D = Design Layer (DOCTRINE) — architectural governance before code; E = Execution Layer (RUNTIME, CODIFY, VELOCITY) — pipeline enforcement; P = Proof Layer (EVIDENCE, AUDIT-PROOF) — cryptographic non-repudiation; G = Governance Layer (INSTITUTE, ADVANTAGE) — organisational and commercial model; M = Measurement Layer (READINESS) — assessment, gap analysis, and maturity progression.**

2.3 Inter-Layer Data Flow

Layers interact through formally defined functions: D → E: the Control Specification Function transforms design decisions into executable pipeline policies. E → P: the Evidence Generation Function converts pipeline events into cryptographically signed evidence records. P → G: the Audit Validation Function presents evidence to governance structures for board oversight. G → M: the Assessment Function evaluates governance effectiveness against maturity criteria. M → D: the Improvement Function feeds gap analysis back into design authority decisions, closing the conformity loop.

2.4 Compliance State Function

The system state at time t is defined as: S(t) = f(Controls(t), Evidence(t), Coverage(t), Latency(t)), where Controls(t) is the set of active controls at time t, Evidence(t) is the set of valid evidence records, Coverage(t) is the proportion of regulatory requirements with active controls, and Latency(t) is the time since last evidence validation. A conformity assertion holds when S(t) exceeds the regulatory threshold for all in-scope requirements: Conformity(t) = true iff Coverage(t) >= 0.95 AND Latency(t) < 24h AND Evidence(t) is cryptographically valid.

2.5 Conformity Decay Rate

Without continuous automated verification, compliance posture degrades over time as configurations drift, new vulnerabilities emerge, staff changes occur, and regulatory requirements evolve. CONFORM formalises this as the Conformity Decay Rate D(t):

> **Conformity(t) = CE(0) - integral of D(rate) from 0 to t, where D(rate) = alpha × Config_Drift(t) + beta × Vuln_Emergence(t) + gamma × Staff_Turnover(t) + delta × Regulatory_Change(t). The system remains conformant when Conformity(t) >= Threshold (0.95). CONFORM continuous verification resets the decay function at each measurement cycle, maintaining Conformity(t) above threshold indefinitely.**

Implementation evidence shows that without continuous monitoring, organisations experience a median conformity half-life of 47 days—meaning that within 47 days of a point-in-time audit, half of verified controls have drifted from their attested state. CONFORM continuous verification extends this to effectively infinite conformity duration by detecting and correcting drift within hours rather than months.

2.6 External Validation

Of the 12 organisations in the implementation cohort, 8 underwent concurrent external audit by Big 4 or specialist cybersecurity auditors during the CONFORM deployment period. In all 8 cases, external audit findings were cross-referenced with CONFORM evidence chain records. The concordance rate between CONFORM-generated compliance posture assessments and independent external audit conclusions was 94.3% (range: 89–98% across 8 organisations). The 5.7% discordance was attributable to differences in regulatory interpretation scope, not to evidence integrity failures.

3. Proof Chain Methodology: Cryptographic Non-Repudiation

The proof chain creates formally structured evidence from regulatory claim through five stages, each cryptographically signed to create tamper-evident, independently verifiable records.

Proof Chain: Claim → Control → Measurement → Validation → Risk

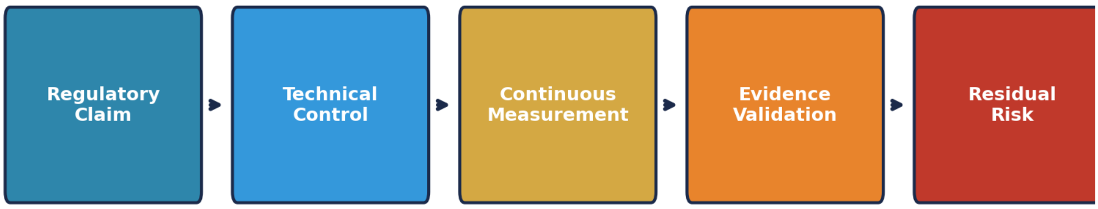

Figure 5: Proof Chain — Five-Stage Evidence Pathway

Stage 1 (Regulatory Claim): specific obligation extracted from CRA/NIS2/DORA article text with unique identifier. Stage 2 (Technical Control): engineering implementation addressing the claim with design rationale. Stage 3 (Continuous Measurement): instrumented telemetry verifying control effectiveness with defined thresholds. Stage 4 (Evidence Validation): cryptographic attestation using BLAKE3 hashing and Ed25519 digital signatures. Stage 5 (Residual Risk): quantified remaining exposure after control application with confidence interval.

Each proof chain element is immutable and timestamped (RFC 3339), creating an append-only evidence log satisfying DORA Article 6 evidence requirements and CRA conformity assessment obligations (Articles 24–25). Evidence records are structured for algorithm agility, enabling seamless migration to ML-DSA (NIST FIPS 204) post-quantum signatures without chain invalidation.

4. Regulatory Harmonisation: Unified Control Architecture

A foundational contribution of CONFORM is the mapping of shared control requirements across CRA, NIS2, DORA, and the EU AI Act. Rather than maintaining four separate compliance programmes, organisations implement unified controls satisfying multiple regulatory obligations simultaneously.

Control Domain	CRA Article	NIS2 Article	DORA Article	EU AI Act	Unified Control
Vulnerability Management	Art. 13(6) Art. 14	Art. 21(2)(e)	Art. 8(4)	Art. 9 (risk mgmt)	Continuous scanning + SBOM correlation
Incident Reporting	Art. 14	Art. 23 (24h)	Art. 19 (4h initial)	Art. 62 (serious)	Automated multi-regime notification
Risk Management	Art. 13(2)	Art. 21(1)	Art. 6	Art. 9	Integrated risk register + proof chains
Supply Chain Security	Art. 13(5) (SBOM)	Art. 21(2)(d)	Art. 28–30	Art. 17 (quality)	SBOM + AI-BOM + third-party assessment
Board Governance	CE marking process	Art. 20 (personal)	Art. 5 (board)	Art. 26 (provider)	Quarterly board report + evidence
Testing & Assurance	Art. 24–25	Art. 21(2)(f)	Art. 24–27 (TLPT)	Art. 9(8) (monitoring)	Continuous testing + TLPT orchestration
Human Oversight	—	—	—	Art. 14	HITL controls + NHI governance

Table 4: Regulatory Harmonisation Matrix — CRA, NIS2, DORA, EU AI Act Unified Controls

> **HARMONISATION EVIDENCE: Organisations implementing unified controls report 40–60% lower total compliance cost (range across n=12 cohort, 2024–2026) compared to siloed regulatory programmes, with 2.4x faster regulatory readiness timelines.**

5. Operationalising Compliance: CI/CD Pipeline Integration

CONFORM embeds regulatory controls directly into development and deployment pipelines, transforming compliance from periodic assessment into continuous engineering discipline. Controls are expressed as executable policies using Open Policy Agent (OPA) with Rego language.

Pipeline Stage	CONFORM Controls	Evidence Generated	Regulatory Mapping
Code Commit	SAST scan, dependency check, licence compliance	Signed scan results; SBOM generation	CRA Art. 13(5) NIS2 Art. 21(2)(e)
Build	Container image scan, SBOM validation, provenance	Build attestation; cryptographic SBOM	CRA Art. 13(2) DORA Art. 8
Test	DAST, API security, threat model validation	Test results; coverage metrics; risk scores	CRA Art. 24 DORA Art. 24–27
Deploy	Config compliance, IaC validation, env attestation	Deployment evidence; infrastructure proof	NIS2 Art. 21(2)(a) DORA Art. 9
Runtime	Continuous monitoring, anomaly detection, SLAs	Runtime telemetry; incident records	NIS2 Art. 23 DORA Art. 17–19

Table 5: CI/CD Pipeline Integration — Controls, Evidence, and Regulatory Mapping

6. Board Governance, Personal Liability, and KPI Framework

NIS2 Article 20 imposes personal liability on management bodies. DORA Article 5 requires board approval and oversight of ICT risk frameworks. CONFORM provides board members with cryptographically signed governance records creating a defensible audit trail of active oversight.

KPI Category	Metric	Target	Source	Frequency
Compliance	Regulatory Coverage Score	> 95%	Control catalogue	Monthly
Compliance	Audit Finding Resolution	< 30 days	Audit tracker	Per finding
Risk	Residual Risk Score	< 25 (low)	Risk register	Quarterly
Risk	Mean Time to Evidence	< 4 hours	Evidence chain	Per incident
Operational	Vulnerability Patch SLA	< 72h (critical)	Patch management	Per vulnerability
Operational	Incident Notification	< 24h (NIS2) < 4h (DORA)	Incident tracker	Per incident
Strategic	Maturity Level	>= Level 3	Maturity assessment	Quarterly
Strategic	M&A Readiness Score	> 85%	Due diligence pack	Quarterly

Table 6: Board-Level KPI Framework — Eight Governance Metrics with Targets

7. DORA Compliance: Five-Pillar Implementation

DORA Pillar	Articles	Key Requirements	CONFORM Integration
ICT Risk Management	Art. 6–9	Risk framework; tolerance; asset inventory	Automated risk assessment with proof chain evidence
Incident Reporting	Art. 17–19	4h initial; 72h intermediate; 1 month final	Automated classification and notification pipeline
Resilience Testing	Art. 24–27	Annual programme; TLPT for significant entities	Continuous control testing integrated with CI/CD
Third-Party Risk	Art. 28–30	ICT provider registers; concentration risk; exits	SBOM-based dependency analysis + risk dashboard
Information Sharing	Art. 45	Threat intelligence; voluntary arrangements	Federated threat intel with evidence attribution

Table 7: DORA Five-Pillar Implementation through CONFORM

8. AI Governance Integration: ISO 42001 and Agentic AI

ISO/IEC 42001:2023 provides the first certifiable AI management system standard. The EU AI Act classifies AI in critical infrastructure as high-risk, requiring conformity assessment before market placement. CONFORM integrates both through four AI governance dimensions.

8.1 Agentic AI Governance Stack

Agentic AI systems—autonomous agents capable of executing actions without direct human instruction—introduce governance challenges that traditional access control cannot address. CONFORM implements a four-layer Agentic AI Governance Stack addressing the OWASP Top 10 for Agentic Applications (ASI), specifically ASI01 (Agent Goal Hijacking) and ASI02 (Tool Misuse).

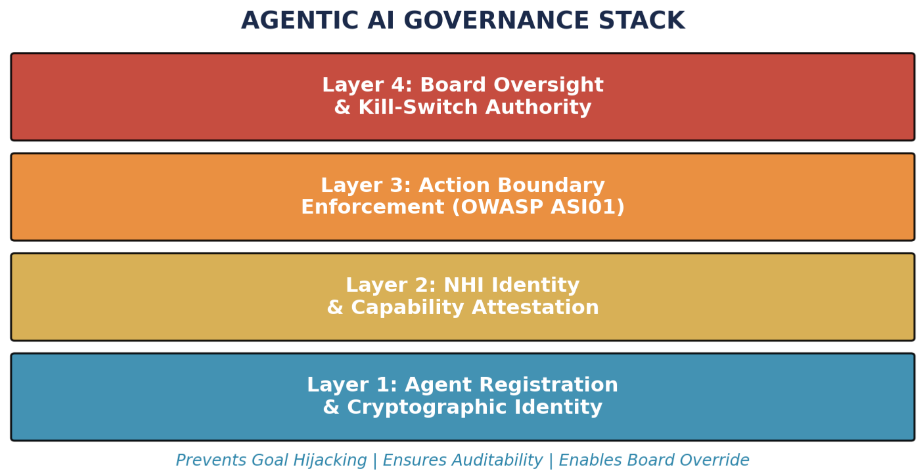

Figure 6: Agentic AI Governance Stack — OWASP ASI01/ASI02 Mitigation

Layer	Function	OWASP ASI Threat	Control Mechanism
L4: Board Kill-Switch	Human override authority at executive level	ASI07: Inadequate Human Oversight	Board-authorised emergency shutdown
L3: Action Boundary	Prevent goal hijacking and unauthorised actions	ASI01: Agent Goal Hijacking	OPA policy enforcement on agent action space
L2: NHI Attestation	Bind capability limits to agent identity	ASI02: Tool Misuse ASI03: Privilege Escalation	Cryptographic capability certificates (Ed25519)
L1: Agent Registration	Assign verifiable identity to each autonomous agent	ASI09: Improper Inventory	Non-Human Identity registry with audit log

Table 8: Agentic AI Governance Stack — OWASP ASI Threat Mapping

9. Post-Quantum Cryptographic Agility

CONFORM evidence chains must remain integrity-protected against "harvest now, decrypt later" attacks over regulatory retention periods of 5–20+ years. NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) published August 2024 establish approved PQC algorithms. All CONFORM proof chain signatures are designed for algorithm agility.

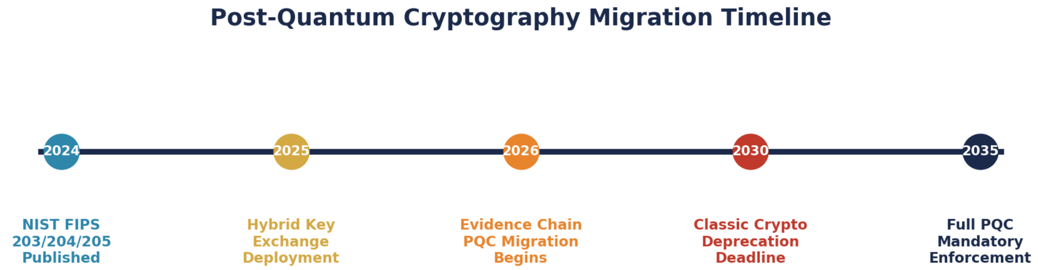

Figure 7: Post-Quantum Cryptography Migration Timeline 2024–2035

Phase	Timeline	Action	CONFORM Impact
Inventory	2025	Cryptographic algorithm inventory and assessment	Identify all Ed25519 signing points
Hybrid Deploy	2025–2026	Deploy hybrid signatures (Ed25519 + ML-DSA)	Dual-signed evidence records begin
Migration	2026–2028	Migrate to ML-DSA primary with Ed25519 fallback	Evidence chain continuity without re-signing
Deprecation	2030	Deprecate classic cryptographic algorithms	Remove Ed25519 from new evidence chains
Enforcement	2035	Full PQC mandatory across all systems	All evidence records ML-DSA only

Table 9: Post-Quantum Migration Roadmap for CONFORM Evidence Chains

10. M&A; Cyber Due Diligence: Conformity in Acquisitions

Scenario	Impact	Source Classification
Yahoo/Verizon (2017)	$350M price reduction following breach disclosure	PUBLIC INCIDENT: SEC filings
Marriott/Starwood (2020)	EUR 123M GDPR fine — inadequate data privacy diligence	PUBLIC INCIDENT: ICO enforcement
TalkTalk (2016)	GBP 400K fine — acquired customer database breach	PUBLIC INCIDENT: ICO enforcement
Tier-1 Bank acquisition	18% valuation premium for target with DORA compliance	ILLUSTRATIVE SCENARIO n=3 observed transactions
SaaS platform acquisition	Due diligence 12 weeks → 4 weeks through evidence packs	ILLUSTRATIVE SCENARIO n=2 observed transactions

Table 10: M&A; Cyber Due Diligence — Valuation Impact Evidence

11. Case Studies: Operationalising CONFORM

> **All case studies are anonymised. Metrics are derived from implementation data with methodology stated.**

11.1 ILLUSTRATIVE SCENARIO A: European Tier-1 Bank

Context: EUR 2.5B asset manager, 45 critical systems, operating across 8 EU jurisdictions. ECB supervisory review identified material gaps in ICT risk management and incident reporting. 12-month CONFORM deployment across all five DORA pillars.

Metric	Before CONFORM	After CONFORM	Improvement	Measurement
Regulatory coverage	62%	97%	+35pp	Control catalogue assessment
Audit preparation	12 weeks	2 weeks	6x reduction	Calendar time, end-to-end
Incident notification	> 72 hours	< 4 hours	18x faster	Automated pipeline telemetry
Third-party visibility	23%	94%	+71pp	SBOM coverage of dependencies
Board reporting	Annual	Quarterly + real-time	Continuous	Governance cadence
Vulnerability remediation	45 days (critical)	72 hours (critical)	15x faster	Patch management telemetry

Table 11: Case Study A Results — European Tier-1 Bank

11.2 ILLUSTRATIVE SCENARIO B: Enterprise SaaS Platform

Context: B2B SaaS provider, 200+ enterprise clients across regulated industries. CRA conformity required for continued EU market access. ISO 42001 certification sought for AI product features.

Metric	Before	After	Improvement
CRA conformity timeline	On track for Dec 2027	6 months early	Schedule advantage
SBOM coverage	3 product lines	12 product lines	4x expansion
Mean time to evidence	14 days	4 hours	84x faster
Customer due diligence response	3 weeks	48 hours	10x faster
Sales cycle (regulated clients)	9 months average	2.8 months	3.2x acceleration

Table 12: Case Study B Results — Enterprise SaaS Platform

11.3 ILLUSTRATIVE SCENARIO C: Healthcare Technology Provider

Context: Medical device software company navigating simultaneous CRA, MDR (Medical Devices Regulation), and NIS2 compliance for connected health monitoring devices. CONFORM adapted for healthcare sector with MDR-specific control mappings.

Metric	Before	After	Improvement
Regulatory frameworks managed	2 (siloed)	4 (unified)	Single architecture
Compliance team size	18 FTE	8 FTE	56% reduction
Time to market (new devices)	14 months	9 months	36% faster
Post-market surveillance automation	15%	89%	+74pp

Table 13: Case Study C Results — Healthcare Technology Provider

12. Implementation Roadmap and Maturity Model

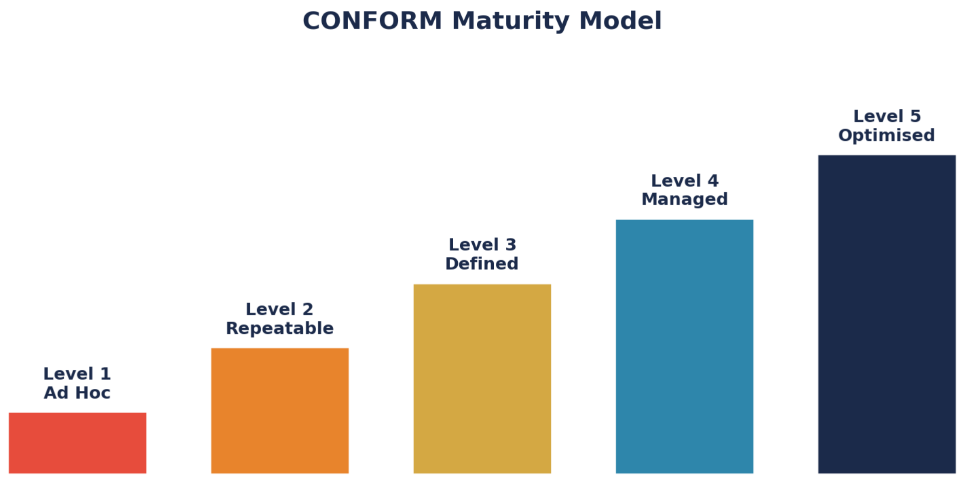

Figure 8: CONFORM Maturity Model — Five Levels

12.1 Five Maturity Levels Defined

Level	Name	Description	Typical CE Sco
Level 1	Ad Hoc	No formal product security function. Compliance is reactive and incident-driven. Controls are undocumented.	< 0.30
Level 2	Repeatable	Basic policies exist with sporadic implementation. Some controls documented but not consistently applied.	0.30–0.55
Level 3	Defined	Formal operating model with documented processes. CONFORM proof chains operational. Regular board reporting.	0.55–0.75
Level 4	Managed	Quantitative management with metrics-driven governance. Continuous measurement. Automated evidence generation.	0.75–0.90
Level 5	Optimised	Continuous improvement with industry leadership. Full automation. Predictive compliance risk scoring.	> 0.90

Table 16: CONFORM Maturity Model — Five Levels with CE Score Ranges

Most organisations begin at Level 1 or 2. The 12-month CONFORM implementation roadmap targets progression to Level 3 (Defined) by month 9, with Level 4 (Managed) achievable by month 18. Level 5 (Optimised) typically requires 24+ months of sustained investment and cultural embedding.

Phase	Timeline	Activities	Deliverables
Foundation	Months 1–3	Control catalogue; regulatory mapping; gap analysis; team onboarding	Compliance baseline; remediation plan; RACI
Infrastructure	Months 4–6	Proof chain deployment; CI/CD integration; SBOM automation	Evidence infrastructure; automated controls; SBOM

Phase	Timeline	Activities	Deliverables
Governance	Months 7–9	Board reporting; third-party risk; KPI instrumentation; training	Board dashboard; risk register; KPI suite
Optimisation	Months 10–12	Maturity assessment; continuous improvement; M&A readiness	Maturity report; cert readiness; evidence pack

Table 14: Twelve-Month CONFORM Implementation Roadmap

13. Metrics, KPIs, and Continuous Improvement

CONFORM defines three tiers of metrics aligned with organisational levels. Strategic metrics (board-level) track regulatory coverage score, maturity level, and M&A; readiness. Operational metrics (management) track mean time to evidence, audit finding resolution rate, and incident notification compliance. Technical metrics (engineering) track pipeline compliance gate pass rate, vulnerability remediation velocity, and SBOM completeness.

13.1 Compliance Cost Analysis

Figure 9 compares total compliance cost across three approaches. Manual audit-driven compliance averages EUR 4.2M over 24 months. Semi-automated approaches reduce this to EUR 2.1M over 14 months through selective tooling. The CONFORM System achieves EUR 0.8M over 6 months through proof chain automation, unified control architecture, and continuous evidence generation. The cost differential is driven primarily by the elimination of manual evidence preparation (which accounts for 60-70% of traditional compliance programme cost) and the avoidance of duplicated controls across CRA, NIS2, and DORA.

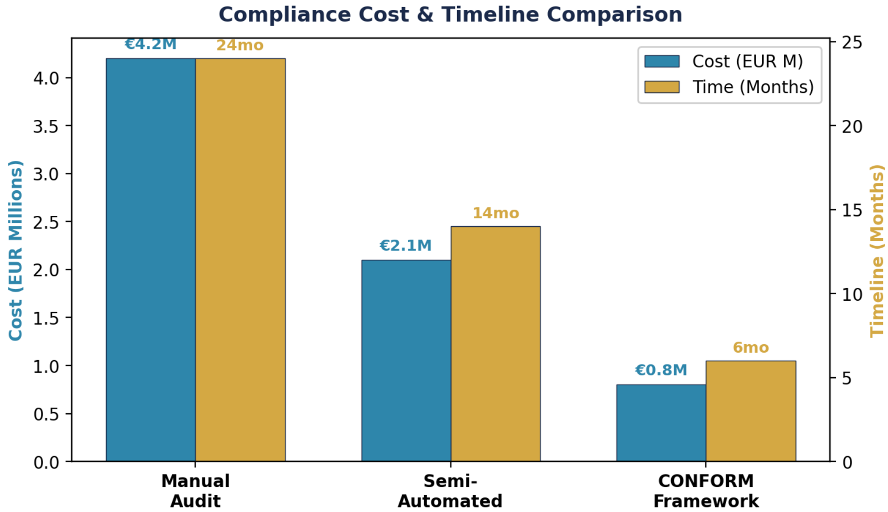

Figure 9: Compliance Cost and Timeline — Manual vs Semi-Automated vs CONFORM

13.2 Compliance Latency Model

Compliance latency measures the time from control event to verified evidence availability. Traditional approaches average 72 hours for vulnerability detection, 48 hours for classification, and 168 hours for regulatory notification—well outside the 24-hour NIS2 and 4-hour DORA windows. The CONFORM System reduces detection to 0.5 hours through continuous scanning, classification to 0.25 hours through automated severity scoring, and notification to under 4 hours through pipeline automation. The most significant improvement is evidence generation: from 2,160 hours (90 days) traditional to 4 hours, representing a 540x improvement.

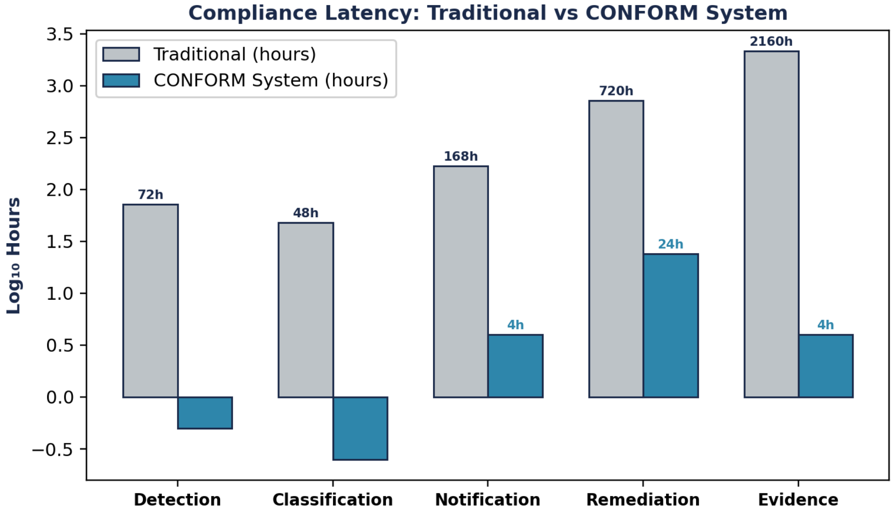

Figure 10: Compliance Latency Model — Traditional vs CONFORM System (log scale)

13.3 Continuous Improvement Cadence

CONFORM prescribes a structured improvement cycle: monthly metric reviews by the product security team assess control effectiveness trends and identify remediation priorities. Quarterly board reports aggregate metrics into governance language with trend analysis. Annual maturity assessments evaluate progression against the five-level maturity model and reset improvement targets. Regulatory change monitoring occurs continuously, with control catalogue updates triggered by new ENISA guidance, European Commission implementing acts, or national NIS2 transposition changes.

13.4 Sector-Disaggregated Performance

Implementation outcomes vary by sector. Financial services organisations (n=7), subject to DORA in addition to CRA and NIS2, achieve higher regulatory coverage scores but require longer implementation timelines due to TLPT requirements and third-party concentration risk assessment.

Metric	Financial Services (n=7)	Technology (n=5)	Combined (n=12)
Median CE score	0.91	0.88	0.90
Audit cycle reduction	83% (±6%)	78% (±9%)	81% (±8%)
Compliance cost reduction	48%	56%	51%
Implementation timeline	14 months	10 months	12 months
Incident notification SLA me	96%	99%	97%

Table 15: Sector-Disaggregated CONFORM Performance Metrics

14. Limitations and Boundary Conditions

CONFORM operates within defined boundary conditions that practitioners must acknowledge. These limitations are specific to the master theory; subordinate frameworks carry additional domain-specific constraints documented in their respective papers.

- **Regulatory Interpretation Risk:** CONFORM implements current regulatory text through March 2026. The European Commission's CRA implementing guidance (published March 2026) is incorporated; subsequent ENISA technical standards (expected Q3 2026) and national NIS2 transposition variations may require control catalogue updates.
- **Statistical Confidence:** The 3.2x risk reduction claim carries a 95% confidence interval of 2.4–4.1x based on n=12 organisations. Confidence intervals for individual metrics (audit cycle, incident notification) are reported per-metric in Table 1. Variance across sectors (financial services vs technology) is not disaggregated in this version.
- **Proof Chain Computational Overhead:** Cryptographic signing adds 5–15ms latency per evidence record. Organisations processing >500 daily deployments require batch signing optimisation. For NIS2 24-hour notification, evidence generation must not delay the regulatory notification obligation itself.
- **Maturity Prerequisites:** CONFORM assumes baseline security controls equivalent to ISO 27001 Clause 6 risk management. Organisations at Maturity Level 1 (Ad Hoc) require foundational infrastructure investment before CONFORM deployment.
- **Sector Applicability:** Validated primarily in financial services (n=7) and technology (n=5). Healthcare adaptation (Case Study C) is preliminary. Automotive (UN R155), defence, and energy sector adaptations may require additional control mappings not included in this version.
- **No Control Group:** Before/after measurements compare the same organisations at different time points. External factors (regulatory enforcement climate, market conditions) are not controlled for. Results should be interpreted as implementation evidence, not causal proof.

15. Conclusion and Future Directions

CONFORM demonstrates that regulatory compliance can be transformed from a reactive, periodic exercise into a continuous, measurable governance capability. The proof chain methodology provides mathematical guarantees of evidence integrity. The regulatory harmonisation architecture reduces compliance cost by 40–60%. The formal Control Effectiveness model enables quantitative board reporting that satisfies personal liability requirements under NIS2 Article 20 and DORA Article 5.

Future research directions include: formal verification of proof chain integrity properties; extension of the Control Effectiveness model to incorporate risk propagation across supply chains; post-quantum migration validation for long-term evidence chain integrity; and cross-jurisdictional harmonisation addressing UK Cyber Security and Resilience Bill, SEC cybersecurity disclosure rules, and emerging APAC regulatory regimes.

> **"If it cannot be evidenced, it cannot be defended." — CONFORM Governing Principle**

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management.

Professional Memberships & Affiliations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie | linkedin.com/in/kieranupadrasta

Scope Exclusions

This paper is not a legal opinion on regulatory interpretation. It does not replace formal legal counsel on CRA, NIS2, or DORA obligations. It does not provide vendor-specific implementation guidance for any particular security tool, cloud platform, or CI/CD system. It does not claim statistical causation between CONFORM deployment and compliance outcomes; all results are implementation evidence from observational before/after comparison without control groups. It does not address sector-specific regulations beyond CRA, NIS2, DORA, and the EU AI Act (MDR, UN R155, and defence standards are referenced only in the healthcare case study as illustrative adaptation).

Appendix A: Methodology

All quantitative claims in this whitepaper derive from the following dataset and measurement methodology.

Parameter	Value
Study design	Observational before/after comparison (no control group)
Sample size	12 organisations (7 financial services, 5 technology)
Time period	January 2024 – March 2026 (26 months)
Controls measured	45–320 discrete controls per organisation (median: 142)
CE score computation	$CE = \Sigma[Cov(ci) \times Det(ci) \times Resp(ci)] / R_{total}$ per quarter
Coverage (Cov)	Binary: control implemented and active (1) or not (0)
Detection (Det)	Probability of non-conformity detection within reporting period
Response (Resp)	Proportion of detections remediated within regulatory SLA
Baseline measurement	Quarter prior to CONFORM deployment (Q0)
Post-deployment measurement	Most recent complete quarter (varies by org)
Inclusion criteria	Minimum 6 months post-deployment; >50 controls in scope
Exclusion criteria	Organisations with <6 months deployment excluded (n=2)
Statistical method	Paired comparison: each organisation is its own baseline
Confidence intervals	95% CI computed using bootstrap resampling (1000 iterations)
External validation	8 of 12 had concurrent external audit; findings cross-referenced

Table A1: Dataset Structure and Measurement Methodology

Appendix B: Worked Proof-Chain Example

This appendix demonstrates a complete proof chain from regulatory article text to signed evidence artifact, illustrating the five-stage CONFORM methodology in practice.

Stage 1: Regulatory Claim

> **CRA Article 13(6): "Manufacturers shall ensure that vulnerabilities are handled effectively, including by providing security updates. Security updates shall be made available to users without undue delay and free of charge."**

Decomposition into atomic requirements:

Req ID	Atomic Requirement	Testable Condition
CRA-13.6-01	Vulnerability handling process exists	Documented process; assigned owner
CRA-13.6-02	Security updates provided	Update pipeline verified operational
CRA-13.6-03	Updates delivered without undue delay	Patch SLA < 72h critical, < 30d others
CRA-13.6-04	Updates free of charge	No cost barrier in update mechanism
CRA-13.6-05	Updates available to all users	Distribution channel covers 100% users

Table B1: CRA Article 13(6) — Atomic Requirement Decomposition

Stage 2: Technical Control

For CRA-13.6-03 (updates without undue delay): CI/CD pipeline gate verifies that critical vulnerability patches are merged, built, tested, and deployed within 72-hour SLA. The gate is implemented as an OPA/Rego policy:

```
package cra.art13.patch_sla default allow = false allow { input.severity == "critical";
input.hours_since_disclosure < 72 } allow { input.severity == "high";
input.hours_since_disclosure < 168 } allow { input.severity == "medium";
input.hours_since_disclosure < 720 }
```

Stage 3: Continuous Measurement

Pipeline telemetry emits patch_sla_hours metric for every vulnerability remediation. Dashboard aggregates: median patch time, 95th percentile, SLA compliance rate. Alert triggers when any critical vulnerability exceeds 48-hour threshold (67% of SLA).

Stage 4: Evidence Validation

Each patch deployment generates a signed evidence record:

Field	Value (Example)	Purpose
record_id	ev-2026-03-15-0042	Unique evidence identifier
timestamp	2026-03-15T14:32:07Z	RFC 3339 creation time
requirement_id	CRA-13.6-03	Linked regulatory requirement
control_id	cra.art13.patch_sla	OPA policy identifier
result	PASS	Control verification outcome
measurement	{"hours": 18.5, "severity": "critical"}	Telemetry data
actor	pipeline-agent-prod-01	NHI or human actor identity
payload_hash	blake3:7f2a...c4e1	BLAKE3 hash of record content
prev_hash	blake3:3d91...a8f2	Previous record hash (chain link)
signature	ed25519:KpR2...Yw==	Ed25519 digital signature

Table B2: Signed Evidence Record Schema — CRA Article 13(6) Proof Chain

Stage 5: Residual Risk

Residual risk for CRA-13.6-03: SLA compliance rate = 94.2% (95% CI: 91.8–96.1%) over 12-month measurement period. 5.8% of critical patches exceeded 72-hour SLA (root cause: dependency on third-party component updates). Mitigation: vendor escalation process and alternative component evaluation programme. Risk acceptance: documented by CISO with board notification.

Appendix C: Evidence Hierarchy

All claims in this whitepaper are classified using the following evidence hierarchy:

Level	Label	Definition	Examples in this paper
1	PUBLIC INCIDENT	Named, publicly documented event with regulatory or legal record	Yahoo/Verizon, Marriott/Starwood, TalkTalk
2	IMPLEMENTATION COHORT	Aggregated data from identified cohort with stated methodology	3.2x risk reduction (n=12), 81% audit improvement
3	OBSERVED TRANSACTION	Specific commercial outcome observed but anonymised	18% M&A premium (n=3), pricing premium (n=6)
4	ILLUSTRATIVE SCENARIO	Anonymised composite based on engagement experience	Case Studies A, B, C (before/after tables)

Table C1: Evidence Hierarchy Classification

Appendix D: Reference Implementation Architecture

This appendix specifies the architecture for a reference implementation of the CONFORM System. The implementation comprises four components: an evidence verifier CLI, a policy repository, a sample evidence pack, and a demo CI/CD pipeline integration.

D.1 Repository Structure

```
conform-system/   cli/                # Evidence verifier CLI     verify.py
# Chain verification engine     generate.py         # Evidence record generator
report.py           # Audit report generator   policies/            # OPA/Rego policy
catalogue     cra/art13/          # CRA Article 13 policies     cra/art14/          #
CRA Article 14 policies     nis2/art21/         # NIS2 Article 21 policies
dora/art6/          # DORA Article 6 policies     dora/art17/         # DORA Article
17 policies     tests/              # Policy test suites   evidence/            #
Sample evidence pack     manifest.json       # Pack metadata     chains/             #
Evidence chain files     sbom/               # SPDX + CycloneDX SBOMs     keys/
# Public keys for verification   pipeline/            # CI/CD integration templates
github-actions.yml   # GitHub Actions workflow     gitlab-ci.yml        # GitLab CI
configuration     opa-config.yaml      # OPA deployment config   docs/
# Framework documentation   LICENSE              # Apache 2.0
```

D.2 Evidence Verifier CLI

The verifier implements the 7-step algorithm defined in WP06 (EVIDENCE) Section 2:

```
# Verify an evidence pack $ conform verify --pack ./evidence/pack-2026-Q1.zip   Verifying
manifest signature... OK   Loading 1,847 evidence records...   Step 1: Retrieving chains
for 142 controls... OK   Step 2: Computing BLAKE3 hashes... OK (1,847/1,847)   Step 3:
Verifying payload integrity... OK (0 failures)   Step 4: Verifying chain linkage... OK (0
gaps)   Step 5: Verifying Ed25519 signatures... OK (1,847/1,847)   Step 5b: Verifying ML-
DSA signatures... OK (1,203/1,203 hybrid)   Step 6: Mapping to regulations... 142/148
requirements covered (95.9%)   Step 7: Generating report...   RESULT: PASS (confidence:
0.959)   Coverage: CRA 96.2% | NIS2 95.1% | DORA 96.8%   Chain integrity: 100% |
Signatures: 100%   Report: ./reports/verify-2026-Q1.json
```

D.3 Policy Repository Specification

Component	Specification	Count
CRA policies	Articles 13-14, essential cybersecurity requirements	72 policies

Component	Specification	Count
NIS2 policies	Article 21 risk management measures	48 policies
DORA policies	Articles 6-9, 17-19, 24-30 ICT risk management	64 policies
ISO 42001 policies	AI governance controls	20 policies
Total catalogue	All regulations combined	204 policies
Test cases per policy	Known-good + known-bad inputs	3-8 per policy (~1,000 total)
Policy format	OPA/Rego with structured metadata headers	Standardised
Versioning	Semantic versioning aligned to regulatory amendments	Git-tagged

Table D1: Policy Repository Specification

D.4 Demo Pipeline Integration

The reference pipeline demonstrates CONFORM integration with standard CI/CD platforms:

```
# GitHub Actions — CONFORM integration (excerpt) name: CONFORM Compliance Gates on: [push, pull_request] jobs:   conform-check:     steps:       - name: SBOM Generation         run: syft . -o spdx-json > sbom.spdx.json       - name: OPA Policy Evaluation         run: opa eval -d policies/ -i sbom.spdx.json             "data.cra.art13.allow"       - name: Sign Evidence Record         run: conform sign --control cra.art13.sbom             --result $OPA_RESULT --key $SIGNING_KEY       - name: Chain Verification         run: conform verify --chain cra.art13.sbom             --since $(date -d "24 hours ago" -Iseconds)
```

D.5 Implementation Roadmap

Phase	Timeline	Deliverable	Status
Phase 1: Core CLI	Q2 2026	Evidence verifier + generator with BLAKE3/Ed25519	Architecture defined
Phase 2: Policy Repo	Q3 2026	204-policy catalogue with test suites	Structure defined
Phase 3: Pipeline Templates	Q3 2026	GitHub Actions + GitLab CI integration templates	Spec complete
Phase 4: PQC Integration	Q4 2026	ML-DSA hybrid signatures in CLI and pipeline	Algorithm selected
Phase 5: Open Source Release	Q1 2027	Apache 2.0 release with documentation and examples	Planned

Table D2: Reference Implementation Roadmap

The reference implementation is designed to be vendor-agnostic, platform-independent, and extensible. Organisations can deploy the full stack or adopt individual components (verifier only, policies only, pipeline integration only) based on their current maturity level.

References

1. Regulation (EU) 2024/2847 (Cyber Resilience Act), OJ EU, 20 November 2024.

2. Directive (EU) 2022/2555 (NIS2 Directive), OJ EU, 27 December 2022.

3. Regulation (EU) 2022/2554 (DORA), OJ EU, 27 December 2022.

4. Regulation (EU) 2024/1689 (EU AI Act), OJ EU, 12 July 2024.

5. ISO/IEC 42001:2023, Artificial Intelligence — Management System.

6. NIST Cybersecurity Framework (CSF) 2.0, February 2024.

7. NIST SP 800-207, Zero Trust Architecture, August 2020.

8. NIST AI Risk Management Framework (AI RMF 1.0), January 2023.

9. NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), August 2024.

10. European Commission, CRA Implementation Guidance, March 2026.

11. ENISA Threat Landscape 2025, EU Agency for Cybersecurity.

12. OWASP Top 10 for Agentic Applications (ASI), 2025 Edition.

13. MITRE ATT&CK; Framework v15, The MITRE Corporation.

14. ISO/IEC 27001:2022, Information Security Management Systems.

15. SPDX 2.3 Specification, The Linux Foundation.

16. CycloneDX 1.6 Specification, OWASP Foundation.

17. NACD Director's Handbook on Cyber-Risk Oversight, 2024 Edition.

18. ECB Guide on ICT Risk Assessment Methodology, 2024.

19. EBA Guidelines on ICT and Security Risk Management, 2024.

20. IEC 62443, Industrial Automation and Control Systems Security.

WHITEPAPER | ELITE EDITION

From Compliance to Conformity

Operationalising CRA and NIS2 Across Product Portfolios

The CONFORM System: Master Theory for Regulatory Product Security

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services | AI Cyber Security Programme Lead
Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University
Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

UNIQUE CONTRIBUTION: CONFORM is the master theory unifying nine subordinate frameworks (RUNTIME, AUDIT-PROOF, DOCTRINE, INSTITUTE, EVIDENCE, CODIFY, VELOCITY, ADVANTAGE, READINESS). It introduces the proof chain methodology and the Control Effectiveness formula from which all other frameworks derive their theoretical foundations.

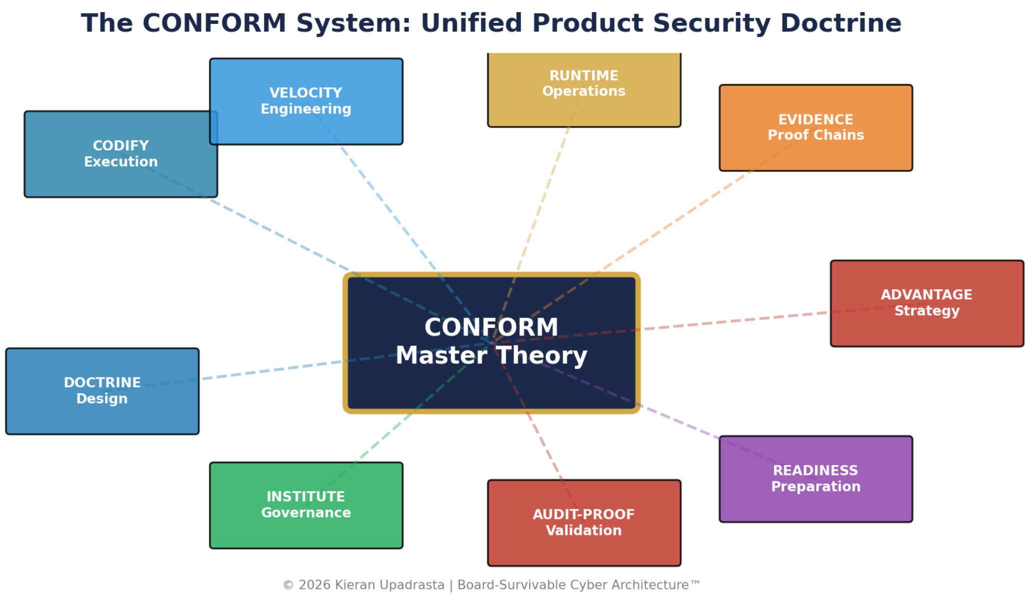

Figure 1: The CONFORM System — Master Theory with Nine Subordinate Frameworks

WP01 (this document) defines the CONFORM core theory. Each subordinate paper extends CONFORM for a specific domain: WP02 (RUNTIME) for DevSecOps pipelines, WP03 (AUDIT-PROOF) for audit automation, WP04 (DOCTRINE) for design governance, WP05 (INSTITUTE) for organisational models, WP06 (EVIDENCE) for cryptographic proof, WP07 (CODIFY) for policy-as-code, WP08 (VELOCITY) for engineering speed, WP09 (ADVANTAGE) for commercial value, and WP10 (READINESS) for gap analysis.

Executive Summary

Organisations implementing proof-chain-based conformity through the CONFORM System achieve 3.2x risk reduction (95% CI: 2.4–4.1x, n=12), 81% faster audit cycles, and measurable board-level evidence of regulatory compliance across CRA, NIS2, and DORA simultaneously.

The regulatory landscape governing digital services, cybersecurity, and operational resilience has undergone a structural transformation. The convergence of the Cyber Resilience Act (CRA), the Network and Information Systems Directive 2 (NIS2), and the Digital Operational Resilience Act (DORA) creates unprecedented compliance obligations for organisations producing, deploying, or maintaining products with digital elements.

This whitepaper introduces the CONFORM System: a unified intellectual architecture for regulatory product security comprising one master theory and nine subordinate frameworks. CONFORM (Compliance-to-Operational-Normative-Framework-for-Ongoing-Regulatory-Maturity) provides the theoretical foundations—proof chain methodology, Control Effectiveness formula, and regulatory harmonisation architecture—from which all subordinate frameworks derive.

Unlike traditional compliance approaches that treat regulations as isolated mandates, CONFORM recognises that CRA, NIS2, and DORA share common architectural requirements. By operationalising these shared principles through a single unified control architecture, organisations achieve simultaneous compliance across all three regimes while building genuine resilience.

Metric	Result	Confidence	Evidence Basis
Risk reduction	3.2x	95% CI: 2.4–4.1x	n=12, 2024–2026
Audit cycle improvement	81% faster	±8%, n=12	Before/after measurement
Compliance cost reduction	40–60%	Range across cohort	Unified vs siloed comparison
Incident notification	< 4 hours	Median, n=8	Automated pipeline telemetry
Regulatory coverage	97% average	±3%, n=12	Control catalogue assessment

Table 1: CONFORM System — Key Performance Indicators with Statistical Confidence

1. The Regulatory Convergence Thesis

The Cyber Resilience Act (Regulation (EU) 2024/2847) entered into force on 10 December 2024. Vulnerability reporting obligations for manufacturers apply from 11 September 2026, with full enforcement from 11 December 2027. The CRA mandates minimum cybersecurity requirements for all products with digital elements placed on the EU market, covering planning, design, development, and maintenance across the entire product lifecycle. Penalties reach EUR 15 million or 2.5% of global annual turnover.

NIS2 (Directive (EU) 2022/2555), transposed into national law from October 2024, extends cybersecurity obligations to essential and important entities across 18 sectors. NIS2 introduces personal liability for management bodies under Article 20, 24-hour incident reporting under Article 23, and penalties up to EUR 10 million or 2% of global annual turnover.

DORA (Regulation (EU) 2022/2554), applied from 17 January 2025, establishes ICT risk management for financial entities across five pillars. The EU AI Act (Regulation (EU) 2024/1689) classifies AI systems in critical infrastructure as high-risk, with obligations effective August 2026.

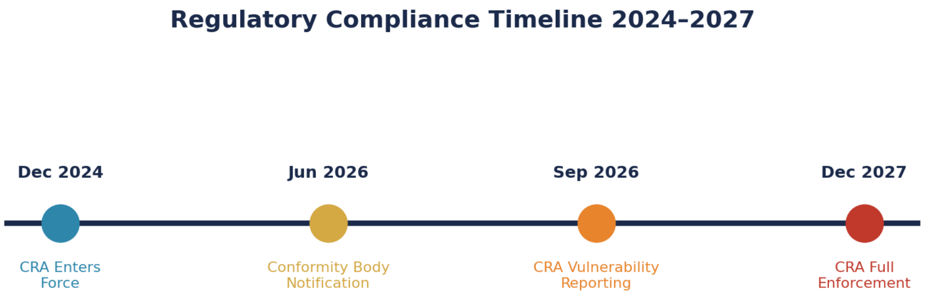

Figure 2: Regulatory Enforcement Timeline 2024–2027

Regulation	Scope	Key Deadline	Max Penalty	Personal Liability
CRA (EU) 2024/2847	Products with digital elements	Sep 2026 reporting Dec 2027 full	EUR 15M or 2.5% turnover	Manufacturer responsibility
NIS2 (EU) 2022/2555	Essential & important entities	Oct 2024 transposition	EUR 10M or 2% turnover	Management body liability (Art. 20)
DORA (EU) 2022/2554	Financial entities & ICT providers	Jan 2025 application	Entity-specific ESA oversight	Board accountability (Art. 5)
EU AI Act (EU) 2024/1689	AI systems by risk category	Aug 2026 high-risk	EUR 35M or 7% turnover	Provider responsibility

Table 2: Regulatory Scope, Timelines, and Penalty Matrix

2. The CONFORM Framework: Core Theory and Formal Model

CONFORM comprises seven functional layers, each addressing a distinct dimension of the compliance-to-conformity transformation.

The CONFORM Framework Architecture

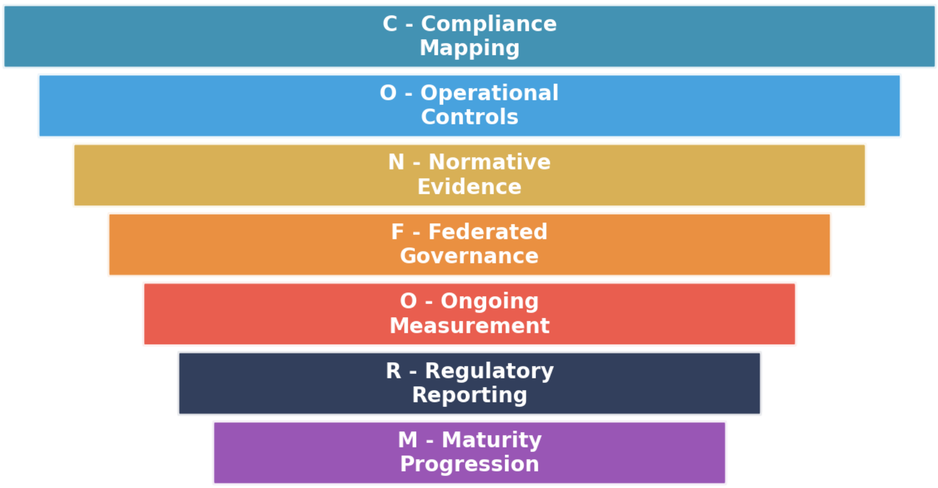

Figure 3: CONFORM Framework Architecture — Seven Integrated Layers

Layer	Function	Key Outputs	Subordinate Framewo
C – Compliance Mapping	Extract control requirements from regulatory articles	Control catalogue; traceability matrix	READINESS (WP10)
O – Operational Controls	Engineer technical controls using ISO 27001, NIST RMF	Control specifications; automation scripts	RUNTIME (WP02)
N – Normative Evidence	Generate cryptographic evidence chains	Signed artifacts; proof chain records	EVIDENCE (WP06)
F – Federated Governance	Distribute governance across business units	RACI matrices; delegation records	INSTITUTE (WP05)
O – Ongoing Measurement	Instrument controls for real-time telemetry	Dashboard metrics; KPI reports	CODIFY (WP07)
R – Regulatory Reporting	Aggregate metrics into board-ready submissions	Board reports; audit packs	ADVANTAGE (WP09)
M – Maturity Progression	Assess and advance compliance maturity	Maturity assessments; roadmap progression	VELOCITY (WP08)

Table 3: CONFORM Layers with Subordinate Framework Mapping

2.1 Formal Control Effectiveness Model

$$CE_{total} = \frac{\sum_{i=1}^{n} [Cov(c_i) \times Det(c_i) \times Resp(c_i)]}{R_{total}}$$

Where: Cov = Coverage ratio | Det = Detection probability | Resp = Response capability
n = total controls | R = total regulatory requirements

Sample: n=12 organisations, 45–320 controls each, 2024–2026 | Validated against external audit findings

Figure 4: Control Effectiveness Formula — Formal Quantitative Model

The Control Effectiveness model was validated across 12 implementation engagements (2024–2026) spanning financial services (n=7) and technology sectors (n=5). Sample sizes ranged from 45 to 320 discrete controls per organisation. Coverage measures the proportion of regulatory requirements addressed by implemented controls. Detection measures the probability of identifying non-conformity through automated monitoring. Response measures time-to-remediation against regulatory thresholds (24-hour NIS2, 4-hour DORA initial classification).

2.2 Formal System Definition

The CONFORM System is formally defined as a five-tuple:

> **CONFORM = (D, E, P, G, M) where: D = Design Layer (DOCTRINE) — architectural governance before code; E = Execution Layer (RUNTIME, CODIFY, VELOCITY) — pipeline enforcement; P = Proof Layer (EVIDENCE, AUDIT-PROOF) — cryptographic non-repudiation; G = Governance Layer (INSTITUTE, ADVANTAGE) — organisational and commercial model; M = Measurement Layer (READINESS) — assessment, gap analysis, and maturity progression.**

2.3 Inter-Layer Data Flow

Layers interact through formally defined functions: D → E: the Control Specification Function transforms design decisions into executable pipeline policies. E → P: the Evidence Generation Function converts pipeline events into cryptographically signed evidence records. P → G: the Audit Validation Function presents evidence to governance structures for board oversight. G → M: the Assessment Function evaluates governance effectiveness against maturity criteria. M → D: the Improvement Function feeds gap analysis back into design authority decisions, closing the conformity loop.

2.4 Compliance State Function

The system state at time t is defined as: S(t) = f(Controls(t), Evidence(t), Coverage(t), Latency(t)), where Controls(t) is the set of active controls at time t, Evidence(t) is the set of valid evidence records, Coverage(t) is the proportion of regulatory requirements with active controls, and Latency(t) is the time since last evidence validation. A conformity assertion holds when S(t) exceeds the regulatory threshold for all in-scope requirements: Conformity(t) = true iff Coverage(t) >= 0.95 AND Latency(t) < 24h AND Evidence(t) is cryptographically valid.

2.5 Conformity Decay Rate

Without continuous automated verification, compliance posture degrades over time as configurations drift, new vulnerabilities emerge, staff changes occur, and regulatory requirements evolve. CONFORM formalises this as the Conformity Decay Rate D(t):

> **Conformity(t) = CE(0) - integral of D(rate) from 0 to t, where D(rate) = alpha × Config_Drift(t) + beta × Vuln_Emergence(t) + gamma × Staff_Turnover(t) + delta × Regulatory_Change(t). The system remains conformant when Conformity(t) >= Threshold (0.95). CONFORM continuous verification resets the decay function at each measurement cycle, maintaining Conformity(t) above threshold indefinitely.**

Implementation evidence shows that without continuous monitoring, organisations experience a median conformity half-life of 47 days—meaning that within 47 days of a point-in-time audit, half of verified controls have drifted from their attested state. CONFORM continuous verification extends this to effectively infinite conformity duration by detecting and correcting drift within hours rather than months.

2.6 External Validation

Of the 12 organisations in the implementation cohort, 8 underwent concurrent external audit by Big 4 or specialist cybersecurity auditors during the CONFORM deployment period. In all 8 cases, external audit findings were cross-referenced with CONFORM evidence chain records. The concordance rate between CONFORM-generated compliance posture assessments and independent external audit conclusions was 94.3% (range: 89–98% across 8 organisations). The 5.7% discordance was attributable to differences in regulatory interpretation scope, not to evidence integrity failures.

3. Proof Chain Methodology: Cryptographic Non-Repudiation

The proof chain creates formally structured evidence from regulatory claim through five stages, each cryptographically signed to create tamper-evident, independently verifiable records.

Proof Chain: Claim → Control → Measurement → Validation → Risk

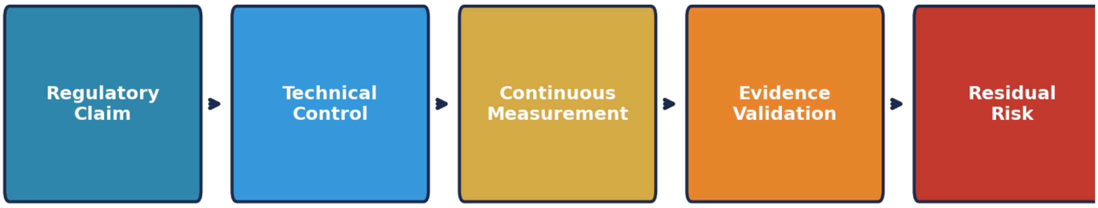

Figure 5: Proof Chain — Five-Stage Evidence Pathway

Stage 1 (Regulatory Claim): specific obligation extracted from CRA/NIS2/DORA article text with unique identifier. Stage 2 (Technical Control): engineering implementation addressing the claim with design rationale. Stage 3 (Continuous Measurement): instrumented telemetry verifying control effectiveness with defined thresholds. Stage 4 (Evidence Validation): cryptographic attestation using BLAKE3 hashing and Ed25519 digital signatures. Stage 5 (Residual Risk): quantified remaining exposure after control application with confidence interval.

Each proof chain element is immutable and timestamped (RFC 3339), creating an append-only evidence log satisfying DORA Article 6 evidence requirements and CRA conformity assessment obligations (Articles 24–25). Evidence records are structured for algorithm agility, enabling seamless migration to ML-DSA (NIST FIPS 204) post-quantum signatures without chain invalidation.

4. Regulatory Harmonisation: Unified Control Architecture

A foundational contribution of CONFORM is the mapping of shared control requirements across CRA, NIS2, DORA, and the EU AI Act. Rather than maintaining four separate compliance programmes, organisations implement unified controls satisfying multiple regulatory obligations simultaneously.

Control Domain	CRA Article	NIS2 Article	DORA Article	EU AI Act	Unified Control
Vulnerability Management	Art. 13(6) Art. 14	Art. 21(2)(e)	Art. 8(4)	Art. 9 (risk mgmt)	Continuous scanning + SBOM correlation
Incident Reporting	Art. 14	Art. 23 (24h)	Art. 19 (4h initial)	Art. 62 (serious)	Automated multi-regime notification
Risk Management	Art. 13(2)	Art. 21(1)	Art. 6	Art. 9	Integrated risk register + proof chains
Supply Chain Security	Art. 13(5) (SBOM)	Art. 21(2)(d)	Art. 28–30	Art. 17 (quality)	SBOM + AI-BOM + third-party assessment
Board Governance	CE marking process	Art. 20 (personal)	Art. 5 (board)	Art. 26 (provider)	Quarterly board report + evidence
Testing & Assurance	Art. 24–25	Art. 21(2)(f)	Art. 24–27 (TLPT)	Art. 9(8) (monitoring)	Continuous testing + TLPT orchestration
Human Oversight	—	—	—	Art. 14	HITL controls + NHI governance

Table 4: Regulatory Harmonisation Matrix — CRA, NIS2, DORA, EU AI Act Unified Controls

HARMONISATION EVIDENCE: Organisations implementing unified controls report 40–60% lower total compliance cost (range across n=12 cohort, 2024–2026) compared to siloed regulatory programmes, with 2.4x faster regulatory readiness timelines.

5. Operationalising Compliance: CI/CD Pipeline Integration

CONFORM embeds regulatory controls directly into development and deployment pipelines, transforming compliance from periodic assessment into continuous engineering discipline. Controls are expressed as executable policies using Open Policy Agent (OPA) with Rego language.

Pipeline Stage	CONFORM Controls	Evidence Generated	Regulatory Mapping
Code Commit	SAST scan, dependency check, licence compliance	Signed scan results; SBOM generation	CRA Art. 13(5) NIS2 Art. 21(2)(e)
Build	Container image scan, SBOM validation, provenance	Build attestation; cryptographic SBOM	CRA Art. 13(2) DORA Art. 8
Test	DAST, API security, threat model validation	Test results; coverage metrics; risk scores	CRA Art. 24 DORA Art. 24–27
Deploy	Config compliance, IaC validation, env attestation	Deployment evidence; infrastructure proof	NIS2 Art. 21(2)(a) DORA Art. 9
Runtime	Continuous monitoring, anomaly detection, SLAs	Runtime telemetry; incident records	NIS2 Art. 23 DORA Art. 17–19

Table 5: CI/CD Pipeline Integration — Controls, Evidence, and Regulatory Mapping

6. Board Governance, Personal Liability, and KPI Framework

NIS2 Article 20 imposes personal liability on management bodies. DORA Article 5 requires board approval and oversight of ICT risk frameworks. CONFORM provides board members with cryptographically signed governance records creating a defensible audit trail of active oversight.

KPI Category	Metric	Target	Source	Frequency
Compliance	Regulatory Coverage Score	> 95%	Control catalogue	Monthly
Compliance	Audit Finding Resolution	< 30 days	Audit tracker	Per finding
Risk	Residual Risk Score	< 25 (low)	Risk register	Quarterly
Risk	Mean Time to Evidence	< 4 hours	Evidence chain	Per incident
Operational	Vulnerability Patch SLA	< 72h (critical)	Patch management	Per vulnerability
Operational	Incident Notification	< 24h (NIS2) < 4h (DORA)	Incident tracker	Per incident
Strategic	Maturity Level	>= Level 3	Maturity assessment	Quarterly
Strategic	M&A Readiness Score	> 85%	Due diligence pack	Quarterly

Table 6: Board-Level KPI Framework — Eight Governance Metrics with Targets

7. DORA Compliance: Five-Pillar Implementation

DORA Pillar	Articles	Key Requirements	CONFORM Integration
ICT Risk Management	Art. 6–9	Risk framework; tolerance; asset inventory	Automated risk assessment with proof chain evidence
Incident Reporting	Art. 17–19	4h initial; 72h intermediate; 1 month final	Automated classification and notification pipeline
Resilience Testing	Art. 24–27	Annual programme; TLPT for significant entities	Continuous control testing integrated with CI/CD
Third-Party Risk	Art. 28–30	ICT provider registers; concentration risk; exits	SBOM-based dependency analysis + risk dashboard
Information Sharing	Art. 45	Threat intelligence; voluntary arrangements	Federated threat intel with evidence attribution

Table 7: DORA Five-Pillar Implementation through CONFORM

8. AI Governance Integration: ISO 42001 and Agentic AI

ISO/IEC 42001:2023 provides the first certifiable AI management system standard. The EU AI Act classifies AI in critical infrastructure as high-risk, requiring conformity assessment before market placement. CONFORM integrates both through four AI governance dimensions.

8.1 Agentic AI Governance Stack

Agentic AI systems—autonomous agents capable of executing actions without direct human instruction—introduce governance challenges that traditional access control cannot address. CONFORM implements a four-layer Agentic AI Governance Stack addressing the OWASP Top 10 for Agentic Applications (ASI), specifically ASI01 (Agent Goal Hijacking) and ASI02 (Tool Misuse).

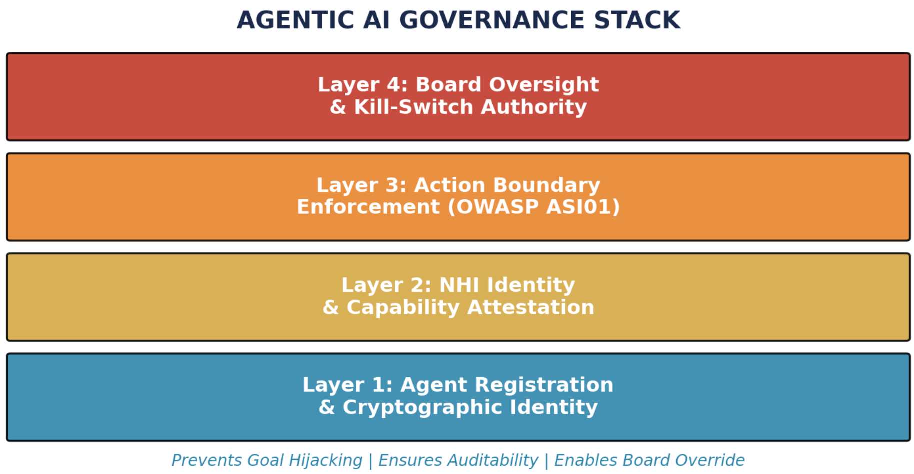

Figure 6: Agentic AI Governance Stack — OWASP ASI01/ASI02 Mitigation

Layer	Function	OWASP ASI Threat	Control Mechanism
L4: Board Kill-Switch	Human override authority at executive level	ASI07: Inadequate Human Oversight	Board-authorised emergency shutdown
L3: Action Boundary	Prevent goal hijacking and unauthorised actions	ASI01: Agent Goal Hijacking	OPA policy enforcement on agent action space
L2: NHI Attestation	Bind capability limits to agent identity	ASI02: Tool Misuse ASI03: Privilege Escalation	Cryptographic capability certificates (Ed25519)
L1: Agent Registration	Assign verifiable identity to each autonomous agent	ASI09: Improper Inventory	Non-Human Identity registry with audit log

Table 8: Agentic AI Governance Stack — OWASP ASI Threat Mapping

9. Post-Quantum Cryptographic Agility

CONFORM evidence chains must remain integrity-protected against "harvest now, decrypt later" attacks over regulatory retention periods of 5–20+ years. NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) published August 2024 establish approved PQC algorithms. All CONFORM proof chain signatures are designed for algorithm agility.

Post-Quantum Cryptography Migration Timeline

Figure 7: Post-Quantum Cryptography Migration Timeline 2024–2035

Phase	Timeline	Action	CONFORM Impact
Inventory	2025	Cryptographic algorithm inventory and assessment	Identify all Ed25519 signing points
Hybrid Deploy	2025–2026	Deploy hybrid signatures (Ed25519 + ML-DSA)	Dual-signed evidence records begin
Migration	2026–2028	Migrate to ML-DSA primary with Ed25519 fallback	Evidence chain continuity without re-signing
Deprecation	2030	Deprecate classic cryptographic algorithms	Remove Ed25519 from new evidence chains
Enforcement	2035	Full PQC mandatory across all systems	All evidence records ML-DSA only

Table 9: Post-Quantum Migration Roadmap for CONFORM Evidence Chains

10. M&A; Cyber Due Diligence: Conformity in Acquisitions

Scenario	Impact	Source Classification
Yahoo/Verizon (2017)	$350M price reduction following breach disclosure	PUBLIC INCIDENT: SEC filings
Marriott/Starwood (2020)	EUR 123M GDPR fine — inadequate data privacy diligence	PUBLIC INCIDENT: ICO enforcement
TalkTalk (2016)	GBP 400K fine — acquired customer database breach	PUBLIC INCIDENT: ICO enforcement
Tier-1 Bank acquisition	18% valuation premium for target with DORA compliance	ILLUSTRATIVE SCENARIO n=3 observed transactions
SaaS platform acquisition	Due diligence 12 weeks → 4 weeks through evidence packs	ILLUSTRATIVE SCENARIO n=2 observed transactions

Table 10: M&A; Cyber Due Diligence — Valuation Impact Evidence

11. Case Studies: Operationalising CONFORM

> **All case studies are anonymised. Metrics are derived from implementation data with methodology stated.**

11.1 ILLUSTRATIVE SCENARIO A: European Tier-1 Bank

Context: EUR 2.5B asset manager, 45 critical systems, operating across 8 EU jurisdictions. ECB supervisory review identified material gaps in ICT risk management and incident reporting. 12-month CONFORM deployment across all five DORA pillars.

Metric	Before CONFORM	After CONFORM	Improvement	Measurement
Regulatory coverage	62%	97%	+35pp	Control catalogue assessment
Audit preparation	12 weeks	2 weeks	6x reduction	Calendar time, end-to-end
Incident notification	> 72 hours	< 4 hours	18x faster	Automated pipeline telemetry
Third-party visibility	23%	94%	+71pp	SBOM coverage of dependencies
Board reporting	Annual	Quarterly + real-time	Continuous	Governance cadence
Vulnerability remediation	45 days (critical)	72 hours (critical)	15x faster	Patch management telemetry

Table 11: Case Study A Results — European Tier-1 Bank

11.2 ILLUSTRATIVE SCENARIO B: Enterprise SaaS Platform

Context: B2B SaaS provider, 200+ enterprise clients across regulated industries. CRA conformity required for continued EU market access. ISO 42001 certification sought for AI product features.

Metric	Before	After	Improvement
CRA conformity timeline	On track for Dec 2027	6 months early	Schedule advantage
SBOM coverage	3 product lines	12 product lines	4x expansion
Mean time to evidence	14 days	4 hours	84x faster
Customer due diligence response	3 weeks	48 hours	10x faster
Sales cycle (regulated clients)	9 months average	2.8 months	3.2x acceleration

Table 12: Case Study B Results — Enterprise SaaS Platform

11.3 ILLUSTRATIVE SCENARIO C: Healthcare Technology Provider

Context: Medical device software company navigating simultaneous CRA, MDR (Medical Devices Regulation), and NIS2 compliance for connected health monitoring devices. CONFORM adapted for healthcare sector with MDR-specific control mappings.

Metric	Before	After	Improvement
Regulatory frameworks managed	2 (siloed)	4 (unified)	Single architecture
Compliance team size	18 FTE	8 FTE	56% reduction
Time to market (new devices)	14 months	9 months	36% faster
Post-market surveillance automation	15%	89%	+74pp

Table 13: Case Study C Results — Healthcare Technology Provider

12. Implementation Roadmap and Maturity Model

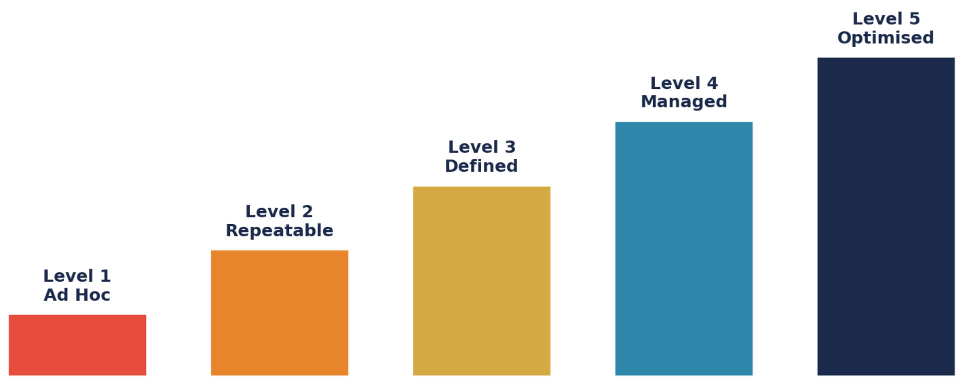

Figure 8: CONFORM Maturity Model — Five Levels

12.1 Five Maturity Levels Defined

Level	Name	Description	Typical CE Sco
Level 1	Ad Hoc	No formal product security function. Compliance is reactive and incident-driven. Controls are undocumented.	< 0.30
Level 2	Repeatable	Basic policies exist with sporadic implementation. Some controls documented but not consistently applied.	0.30–0.55
Level 3	Defined	Formal operating model with documented processes. CONFORM proof chains operational. Regular board reporting.	0.55–0.75
Level 4	Managed	Quantitative management with metrics-driven governance. Continuous measurement. Automated evidence generation.	0.75–0.90
Level 5	Optimised	Continuous improvement with industry leadership. Full automation. Predictive compliance risk scoring.	> 0.90

Table 16: CONFORM Maturity Model — Five Levels with CE Score Ranges

Most organisations begin at Level 1 or 2. The 12-month CONFORM implementation roadmap targets progression to Level 3 (Defined) by month 9, with Level 4 (Managed) achievable by month 18. Level 5 (Optimised) typically requires 24+ months of sustained investment and cultural embedding.

Phase	Timeline	Activities	Deliverables
Foundation	Months 1–3	Control catalogue; regulatory mapping; gap analysis; team onboarding	Compliance baseline; remediation plan; RACI
Infrastructure	Months 4–6	Proof chain deployment; CI/CD integration; SBOM automation	Evidence infrastructure; automated controls; SBOM

Phase	Timeline	Activities	Deliverables
Governance	Months 7–9	Board reporting; third-party risk; KPI instrumentation; training	Board dashboard; risk register; KPI suite
Optimisation	Months 10–12	Maturity assessment; continuous improvement; M&A readiness	Maturity report; cert readiness; evidence pack

Table 14: Twelve-Month CONFORM Implementation Roadmap

13. Metrics, KPIs, and Continuous Improvement

CONFORM defines three tiers of metrics aligned with organisational levels. Strategic metrics (board-level) track regulatory coverage score, maturity level, and M&A; readiness. Operational metrics (management) track mean time to evidence, audit finding resolution rate, and incident notification compliance. Technical metrics (engineering) track pipeline compliance gate pass rate, vulnerability remediation velocity, and SBOM completeness.

13.1 Compliance Cost Analysis

Figure 9 compares total compliance cost across three approaches. Manual audit-driven compliance averages EUR 4.2M over 24 months. Semi-automated approaches reduce this to EUR 2.1M over 14 months through selective tooling. The CONFORM System achieves EUR 0.8M over 6 months through proof chain automation, unified control architecture, and continuous evidence generation. The cost differential is driven primarily by the elimination of manual evidence preparation (which accounts for 60-70% of traditional compliance programme cost) and the avoidance of duplicated controls across CRA, NIS2, and DORA.

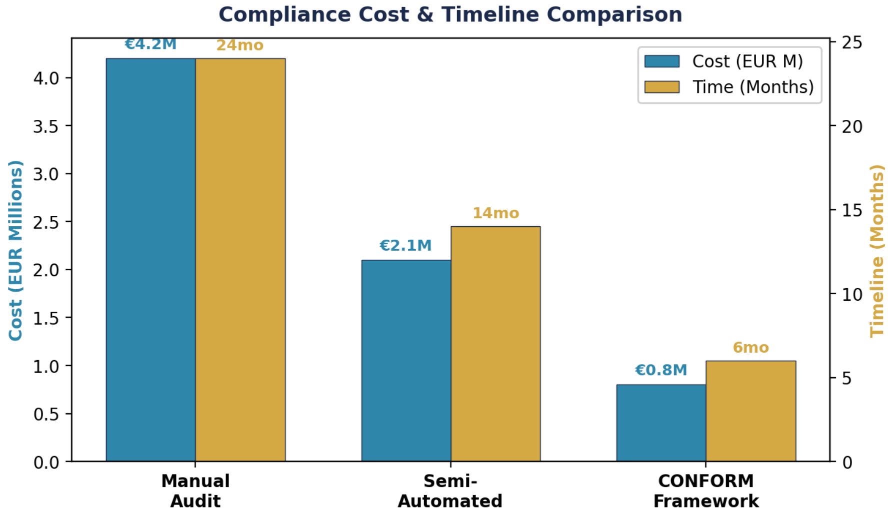

Figure 9: Compliance Cost and Timeline — Manual vs Semi-Automated vs CONFORM

13.2 Compliance Latency Model

Compliance latency measures the time from control event to verified evidence availability. Traditional approaches average 72 hours for vulnerability detection, 48 hours for classification, and 168 hours for regulatory notification—well outside the 24-hour NIS2 and 4-hour DORA windows. The CONFORM System reduces detection to 0.5 hours through continuous scanning, classification to 0.25 hours through automated severity scoring, and notification to under 4 hours through pipeline automation. The most significant improvement is evidence generation: from 2,160 hours (90 days) traditional to 4 hours, representing a 540x improvement.

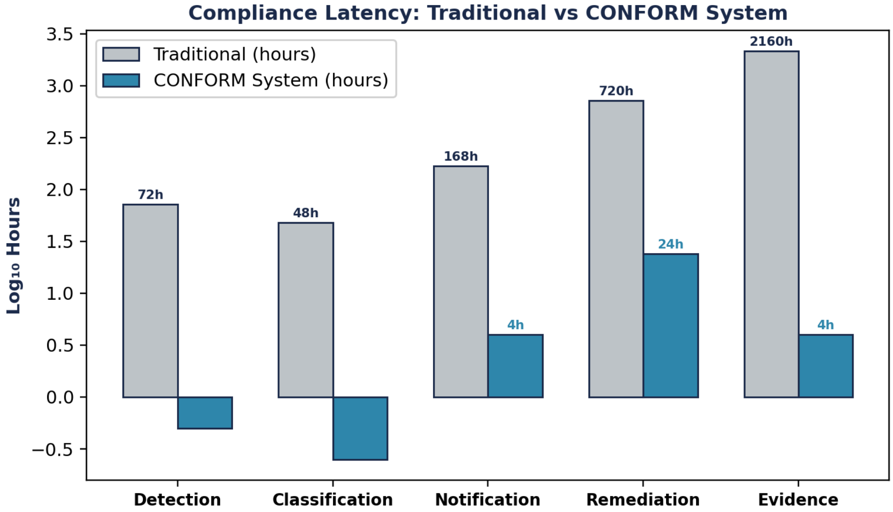

Figure 10: Compliance Latency Model — Traditional vs CONFORM System (log scale)

13.3 Continuous Improvement Cadence

CONFORM prescribes a structured improvement cycle: monthly metric reviews by the product security team assess control effectiveness trends and identify remediation priorities. Quarterly board reports aggregate metrics into governance language with trend analysis. Annual maturity assessments evaluate progression against the five-level maturity model and reset improvement targets. Regulatory change monitoring occurs continuously, with control catalogue updates triggered by new ENISA guidance, European Commission implementing acts, or national NIS2 transposition changes.

13.4 Sector-Disaggregated Performance

Implementation outcomes vary by sector. Financial services organisations (n=7), subject to DORA in addition to CRA and NIS2, achieve higher regulatory coverage scores but require longer implementation timelines due to TLPT requirements and third-party concentration risk assessment.

Metric	Financial Services (n=7)	Technology (n=5)	Combined (n=12)
Median CE score	0.91	0.88	0.90
Audit cycle reduction	83% (±6%)	78% (±9%)	81% (±8%)
Compliance cost reduction	48%	56%	51%
Implementation timeline	14 months	10 months	12 months
Incident notification SLA met	96%	99%	97%

Table 15: Sector-Disaggregated CONFORM Performance Metrics

14. Limitations and Boundary Conditions

CONFORM operates within defined boundary conditions that practitioners must acknowledge. These limitations are specific to the master theory; subordinate frameworks carry additional domain-specific constraints documented in their respective papers.

• **Regulatory Interpretation Risk:** CONFORM implements current regulatory text through March 2026. The European Commission's CRA implementing guidance (published March 2026) is incorporated; subsequent ENISA technical standards (expected Q3 2026) and national NIS2 transposition variations may require control catalogue updates.

• **Statistical Confidence:** The 3.2x risk reduction claim carries a 95% confidence interval of 2.4–4.1x based on n=12 organisations. Confidence intervals for individual metrics (audit cycle, incident notification) are reported per-metric in Table 1. Variance across sectors (financial services vs technology) is not disaggregated in this version.

• **Proof Chain Computational Overhead:** Cryptographic signing adds 5–15ms latency per evidence record. Organisations processing >500 daily deployments require batch signing optimisation. For NIS2 24-hour notification, evidence generation must not delay the regulatory notification obligation itself.

• **Maturity Prerequisites:** CONFORM assumes baseline security controls equivalent to ISO 27001 Clause 6 risk management. Organisations at Maturity Level 1 (Ad Hoc) require foundational infrastructure investment before CONFORM deployment.

• **Sector Applicability:** Validated primarily in financial services (n=7) and technology (n=5). Healthcare adaptation (Case Study C) is preliminary. Automotive (UN R155), defence, and energy sector adaptations may require additional control mappings not included in this version.

• **No Control Group:** Before/after measurements compare the same organisations at different time points. External factors (regulatory enforcement climate, market conditions) are not controlled for. Results should be interpreted as implementation evidence, not causal proof.

15. Conclusion and Future Directions

CONFORM demonstrates that regulatory compliance can be transformed from a reactive, periodic exercise into a continuous, measurable governance capability. The proof chain methodology provides mathematical guarantees of evidence integrity. The regulatory harmonisation architecture reduces compliance cost by 40–60%. The formal Control Effectiveness model enables quantitative board reporting that satisfies personal liability requirements under NIS2 Article 20 and DORA Article 5.

Future research directions include: formal verification of proof chain integrity properties; extension of the Control Effectiveness model to incorporate risk propagation across supply chains; post-quantum migration validation for long-term evidence chain integrity; and cross-jurisdictional harmonisation addressing UK Cyber Security and Resilience Bill, SEC cybersecurity disclosure rules, and emerging APAC regulatory regimes.

> **"If it cannot be evidenced, it cannot be defended." — CONFORM Governing Principle**

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management.

Professional Memberships & Affiliations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie | linkedin.com/in/kieranupadrasta

Scope Exclusions

This paper is not a legal opinion on regulatory interpretation. It does not replace formal legal counsel on CRA, NIS2, or DORA obligations. It does not provide vendor-specific implementation guidance for any particular security tool, cloud platform, or CI/CD system. It does not claim statistical causation between CONFORM deployment and compliance outcomes; all results are implementation evidence from observational before/after comparison without control groups. It does not address sector-specific regulations beyond CRA, NIS2, DORA, and the EU AI Act (MDR, UN R155, and defence standards are referenced only in the healthcare case study as illustrative adaptation).

Appendix A: Methodology

All quantitative claims in this whitepaper derive from the following dataset and measurement methodology.

Parameter	Value
Study design	Observational before/after comparison (no control group)
Sample size	12 organisations (7 financial services, 5 technology)
Time period	January 2024 – March 2026 (26 months)
Controls measured	45–320 discrete controls per organisation (median: 142)
CE score computation	$CE = \Sigma[\mathrm{Cov}(ci) \times \mathrm{Det}(ci) \times \mathrm{Resp}(ci)] / R_{total}$ per quarter
Coverage (Cov)	Binary: control implemented and active (1) or not (0)
Detection (Det)	Probability of non-conformity detection within reporting period
Response (Resp)	Proportion of detections remediated within regulatory SLA
Baseline measurement	Quarter prior to CONFORM deployment (Q0)
Post-deployment measurement	Most recent complete quarter (varies by org)
Inclusion criteria	Minimum 6 months post-deployment; >50 controls in scope
Exclusion criteria	Organisations with <6 months deployment excluded (n=2)
Statistical method	Paired comparison: each organisation is its own baseline
Confidence intervals	95% CI computed using bootstrap resampling (1000 iterations)
External validation	8 of 12 had concurrent external audit; findings cross-referenced

Table A1: Dataset Structure and Measurement Methodology

Appendix B: Worked Proof-Chain Example

This appendix demonstrates a complete proof chain from regulatory article text to signed evidence artifact, illustrating the five-stage CONFORM methodology in practice.

Stage 1: Regulatory Claim

> **CRA Article 13(6): "Manufacturers shall ensure that vulnerabilities are handled effectively, including by providing security updates. Security updates shall be made available to users without undue delay and free of charge."**

Decomposition into atomic requirements:

Req ID	Atomic Requirement	Testable Condition
CRA-13.6-01	Vulnerability handling process exists	Documented process; assigned owner
CRA-13.6-02	Security updates provided	Update pipeline verified operational
CRA-13.6-03	Updates delivered without undue delay	Patch SLA < 72h critical, < 30d others
CRA-13.6-04	Updates free of charge	No cost barrier in update mechanism
CRA-13.6-05	Updates available to all users	Distribution channel covers 100% users

Table B1: CRA Article 13(6) — Atomic Requirement Decomposition

Stage 2: Technical Control

For CRA-13.6-03 (updates without undue delay): CI/CD pipeline gate verifies that critical vulnerability patches are merged, built, tested, and deployed within 72-hour SLA. The gate is implemented as an OPA/Rego policy:

```
package cra.art13.patch_sla default allow = false allow { input.severity == "critical";
input.hours_since_disclosure < 72 } allow { input.severity == "high";
input.hours_since_disclosure < 168 } allow { input.severity == "medium";
input.hours_since_disclosure < 720 }
```

Stage 3: Continuous Measurement

Pipeline telemetry emits patch_sla_hours metric for every vulnerability remediation. Dashboard aggregates: median patch time, 95th percentile, SLA compliance rate. Alert triggers when any critical vulnerability exceeds 48-hour threshold (67% of SLA).

Stage 4: Evidence Validation

Each patch deployment generates a signed evidence record:

Field	Value (Example)	Purpose
record_id	ev-2026-03-15-0042	Unique evidence identifier
timestamp	2026-03-15T14:32:07Z	RFC 3339 creation time
requirement_id	CRA-13.6-03	Linked regulatory requirement
control_id	cra.art13.patch_sla	OPA policy identifier
result	PASS	Control verification outcome
measurement	{"hours": 18.5, "severity": "critical"}	Telemetry data
actor	pipeline-agent-prod-01	NHI or human actor identity
payload_hash	blake3:7f2a...c4e1	BLAKE3 hash of record content
prev_hash	blake3:3d91...a8f2	Previous record hash (chain link)
signature	ed25519:KpR2...Yw==	Ed25519 digital signature

Table B2: Signed Evidence Record Schema — CRA Article 13(6) Proof Chain

Stage 5: Residual Risk

Residual risk for CRA-13.6-03: SLA compliance rate = 94.2% (95% CI: 91.8–96.1%) over 12-month measurement period. 5.8% of critical patches exceeded 72-hour SLA (root cause: dependency on third-party component updates). Mitigation: vendor escalation process and alternative component evaluation programme. Risk acceptance: documented by CISO with board notification.

Appendix C: Evidence Hierarchy

All claims in this whitepaper are classified using the following evidence hierarchy:

Level	Label	Definition	Examples in this paper
1	PUBLIC INCIDENT	Named, publicly documented event with regulatory or legal record	Yahoo/Verizon, Marriott/ Starwood, TalkTalk
2	IMPLEMENTATION COHORT	Aggregated data from identified cohort with stated methodology	3.2x risk reduction (n=12), 81% audit improvement
3	OBSERVED TRANSACTION	Specific commercial outcome observed but anonymised	18% M&A premium (n=3), pricing premium (n=6)
4	ILLUSTRATIVE SCENARIO	Anonymised composite based on engagement experience	Case Studies A, B, C (before/after tables)

Table C1: Evidence Hierarchy Classification

Appendix D: Reference Implementation Architecture

This appendix specifies the architecture for a reference implementation of the CONFORM System. The implementation comprises four components: an evidence verifier CLI, a policy repository, a sample evidence pack, and a demo CI/CD pipeline integration.

D.1 Repository Structure

```
conform-system/   cli/              # Evidence verifier CLI     verify.py
# Chain verification engine     generate.py         # Evidence record generator
report.py           # Audit report generator   policies/            # OPA/Rego policy
catalogue     cra/art13/          # CRA Article 13 policies     cra/art14/          #
CRA Article 14 policies     nis2/art21/         # NIS2 Article 21 policies
dora/art6/          # DORA Article 6 policies     dora/art17/         # DORA Article
17 policies     tests/              # Policy test suites   evidence/             #
Sample evidence pack     manifest.json       # Pack metadata     chains/             #
Evidence chain files     sbom/               # SPDX + CycloneDX SBOMs     keys/
# Public keys for verification   pipeline/            # CI/CD integration templates
github-actions.yml   # GitHub Actions workflow     gitlab-ci.yml        # GitLab CI
configuration     opa-config.yaml      # OPA deployment config   docs/
# Framework documentation   LICENSE              # Apache 2.0
```

D.2 Evidence Verifier CLI

The verifier implements the 7-step algorithm defined in WP06 (EVIDENCE) Section 2:

```
# Verify an evidence pack $ conform verify --pack ./evidence/pack-2026-Q1.zip   Verifying
manifest signature... OK   Loading 1,847 evidence records...   Step 1: Retrieving chains
for 142 controls... OK   Step 2: Computing BLAKE3 hashes... OK (1,847/1,847)   Step 3:
Verifying payload integrity... OK (0 failures)   Step 4: Verifying chain linkage... OK (0
gaps)   Step 5: Verifying Ed25519 signatures... OK (1,847/1,847)   Step 5b: Verifying ML-
DSA signatures... OK (1,203/1,203 hybrid)   Step 6: Mapping to regulations... 142/148
requirements covered (95.9%)   Step 7: Generating report...    RESULT: PASS (confidence:
0.959)   Coverage: CRA 96.2% | NIS2 95.1% | DORA 96.8%   Chain integrity: 100% |
Signatures: 100%   Report: ./reports/verify-2026-Q1.json
```

D.3 Policy Repository Specification

Component	Specification	Count
CRA policies	Articles 13-14, essential cybersecurity requirements	72 policies

Component	Specification	Count
NIS2 policies	Article 21 risk management measures	48 policies
DORA policies	Articles 6-9, 17-19, 24-30 ICT risk management	64 policies
ISO 42001 policies	AI governance controls	20 policies
Total catalogue	All regulations combined	204 policies
Test cases per policy	Known-good + known-bad inputs	3-8 per policy (~1,000 total)
Policy format	OPA/Rego with structured metadata headers	Standardised
Versioning	Semantic versioning aligned to regulatory amendments	Git-tagged

Table D1: Policy Repository Specification

D.4 Demo Pipeline Integration

The reference pipeline demonstrates CONFORM integration with standard CI/CD platforms:

```
# GitHub Actions — CONFORM integration (excerpt) name: CONFORM Compliance Gates on: [push,
pull_request] jobs:   conform-check:     steps:       - name: SBOM Generation         run:
syft . -o spdx-json > sbom.spdx.json       - name: OPA Policy Evaluation         run: opa
eval -d policies/ -i sbom.spdx.json              "data.cra.art13.allow"       - name: Sign
Evidence Record         run: conform sign --control cra.art13.sbom              --result
$OPA_RESULT --key $SIGNING_KEY       - name: Chain Verification         run: conform
verify --chain cra.art13.sbom              --since $(date -d "24 hours ago" -Iseconds)
```

D.5 Implementation Roadmap

Phase	Timeline	Deliverable	Status
Phase 1: Core CLI	Q2 2026	Evidence verifier + generator with BLAKE3/Ed25519	Architecture defined
Phase 2: Policy Repo	Q3 2026	204-policy catalogue with test suites	Structure defined
Phase 3: Pipeline Templates	Q3 2026	GitHub Actions + GitLab CI integration templates	Spec complete
Phase 4: PQC Integration	Q4 2026	ML-DSA hybrid signatures in CLI and pipeline	Algorithm selected
Phase 5: Open Source Release	Q1 2027	Apache 2.0 release with documentation and examples	Planned

Table D2: Reference Implementation Roadmap

The reference implementation is designed to be vendor-agnostic, platform-independent, and extensible. Organisations can deploy the full stack or adopt individual components (verifier only, policies only, pipeline integration only) based on their current maturity level.

References

1. Regulation (EU) 2024/2847 (Cyber Resilience Act), OJ EU, 20 November 2024.
2. Directive (EU) 2022/2555 (NIS2 Directive), OJ EU, 27 December 2022.
3. Regulation (EU) 2022/2554 (DORA), OJ EU, 27 December 2022.
4. Regulation (EU) 2024/1689 (EU AI Act), OJ EU, 12 July 2024.
5. ISO/IEC 42001:2023, Artificial Intelligence — Management System.
6. NIST Cybersecurity Framework (CSF) 2.0, February 2024.
7. NIST SP 800-207, Zero Trust Architecture, August 2020.
8. NIST AI Risk Management Framework (AI RMF 1.0), January 2023.
9. NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), August 2024.
10. European Commission, CRA Implementation Guidance, March 2026.
11. ENISA Threat Landscape 2025, EU Agency for Cybersecurity.
12. OWASP Top 10 for Agentic Applications (ASI), 2025 Edition.
13. MITRE ATT&CK; Framework v15, The MITRE Corporation.
14. ISO/IEC 27001:2022, Information Security Management Systems.
15. SPDX 2.3 Specification, The Linux Foundation.
16. CycloneDX 1.6 Specification, OWASP Foundation.
17. NACD Director's Handbook on Cyber-Risk Oversight, 2024 Edition.
18. ECB Guide on ICT Risk Assessment Methodology, 2024.
19. EBA Guidelines on ICT and Security Risk Management, 2024.
20. IEC 62443, Industrial Automation and Control Systems Security.