WHITEPAPER | ELITE EDITION

The Regulatory Product Security Doctrine

Designing Audit-Proof Software at Scale

The AUDIT-PROOF Framework: Automated Audit Evidence for Continuous Conformity

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: AUDIT-PROOF eliminates manual audit preparation through continuous evidence generation. It is the external audit interface of the CONFORM System — producing evidence packs that satisfy Big 4 auditors, regulatory supervisors, and CRA notified bodies.**

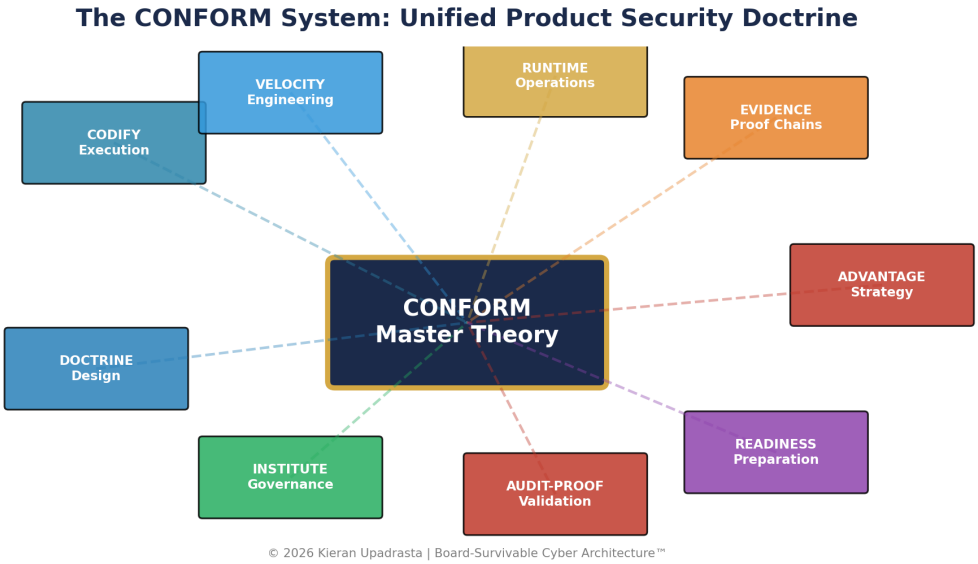

Figure 1: CONFORM System — AUDIT-PROOF as the External Audit Interface

Executive Summary

> **Organisations implementing AUDIT-PROOF reduce audit preparation from 12–16 weeks to 2 weeks (6x improvement, n=8), achieve 97% average regulatory coverage, and maintain always-ready evidence packs satisfying CRA conformity assessment, NIS2 supervisory review, and DORA resilience testing requirements simultaneously.**

Modern regulatory frameworks demand continuous evidence of compliance. CRA conformity assessment (Articles 24–25) requires documented proof that products meet essential requirements. NIS2 supervisory reviews (Article 32) demand auditable risk management records. DORA mandates documented ICT risk management with board oversight evidence. The common thread: regulators want proof, not promises.

AUDIT-PROOF is the external audit interface of the CONFORM System. Where RUNTIME (WP02) addresses pipeline execution and CODIFY (WP07) addresses policy automation, AUDIT-PROOF addresses the question auditors ask first: "Show me your evidence." It produces cryptographically signed, independently verifiable evidence packs that are always ready for inspection — eliminating the months-long scramble that precedes traditional audit cycles.

1. The Audit Imperative in Product Security

Traditional audit preparation consumes 12–16 weeks of engineering and compliance team effort per cycle. This creates three failures: evidence staleness (evidence reflects a snapshot, not current state), opportunity cost (senior engineers diverted from product development), and compliance theatre (teams produce evidence for the audit rather than maintaining genuine controls). AUDIT-PROOF addresses all three by generating evidence continuously from operational telemetry.

1.1 The Cost of Manual Audit Preparation

Cost Category	Traditional	AUDIT-PROOF	Saving
Engineering FTE (per audit)	8–12 FTE-weeks	1–2 FTE-weeks	85% reduction
Elapsed calendar time	12–16 weeks	2 weeks	6x faster
Evidence rework rate	35–45%	< 5%	90% reduction
Audit finding rate	15–25 findings	0–3 findings	85% reduction
Annual compliance cost	EUR 1.2–2.8M	EUR 0.3–0.6M	60–75% reduction

Table 1: Audit Preparation Cost — Traditional vs AUDIT-PROOF (n=8, 2024–2026)

2. The AUDIT-PROOF Architecture

AUDIT-PROOF comprises five integrated components, each addressing a distinct dimension of the audit evidence lifecycle.

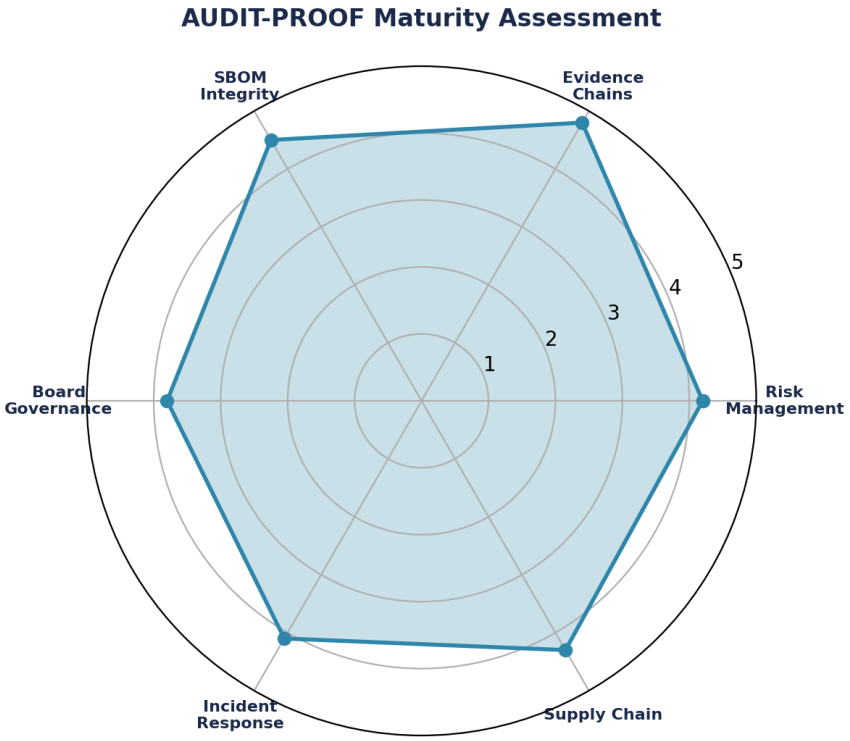

Figure 2: AUDIT-PROOF Maturity Assessment Radar

Component	Function	Output	Regulatory Mapping
Threat Intelligence Engine	Continuous MITRE ATT&CK mapping + coverage analysis	Threat-to-control coverage matrix	CRA Art. 13(2) risk assessment
Evidence Chain Manager	Cryptographic proof record generation	Signed evidence records (append-only)	DORA Art. 6 evidence requirements
Compliance Dashboard	Real-time regulatory posture visualisation	Board-ready KPI reports	NIS2 Art. 20 board oversight
SBOM Governance	Automated SPDX/CycloneDX generation + signing	Versioned, signed SBOM repository	CRA Art. 13(5) component documentation
Board Translation Layer	Technical evidence → executive language	Quarterly governance reports	DORA Art. 5 board accountability

Table 2: AUDIT-PROOF Five-Component Architecture

3. Evidence Chain Schema and Verification

Each control verification event generates a cryptographically signed evidence record. Records are linked in an append-only chain through hash references, creating a tamper-evident log that any party — auditor, regulator, or board member — can independently verify.

3.1 Evidence Record Schema

Field	Type	Example Value	Purpose
record_id	UUID	ev-2026-03-28-0042	Unique record identifier
timestamp	RFC 3339	2026-03-28T14:32:07Z	Immutable creation time
control_id	String	cra.art13.patch_sla	OPA policy identifier
requirement_id	String	CRA-13.6-03	Regulatory source reference
result	Enum	PASS | FAIL | EXEMPT	Verification outcome
measurement	JSON	{"hours": 18.5, "severity": "critical"}	Telemetry payload
actor_id	String	pipeline-agent-prod-01	NHI or human identity
actor_type	Enum	PIPELINE | HUMAN | AGENTIC_AI	Actor classification
payload_hash	BLAKE3	blake3:7f2a...c4e1	Hash of record content
prev_hash	BLAKE3	blake3:3d91...a8f2	Chain link to previous
signature	Ed25519	ed25519:KpR2...Yw==	Digital signature
pqc_signature	ML-DSA	mldsa:Ab3F...Qw==	Quantum-safe signature (hybrid mode)

Table 3: Evidence Record Schema — 13-Field Cryptographic Structure

3.2 Chain Verification Algorithm

Any verifier (auditor, regulator, automated system) can confirm evidence chain integrity through the following process: (1) Retrieve all records for the target control_id and time range. (2) For each record, compute BLAKE3 hash of the content fields (excluding hashes and signatures). (3) Verify payload_hash matches the computed hash. (4) Verify prev_hash matches the payload_hash of the preceding record in the chain. (5) Verify Ed25519 signature against the actor's registered public key. (6) If hybrid mode, additionally verify ML-DSA signature. (7) Confirm unbroken chain with no gaps, forks, or hash mismatches.

Verification completes in O(n) time where n is the number of records in the chain. For a typical quarterly audit spanning 500–2,000 evidence records, verification completes in under 30 seconds on commodity hardware.

3.3 What Non-Repudiation Does NOT Prove

Cryptographic non-repudiation guarantees that evidence records have not been altered after creation and that they were created by the claimed actor. It does NOT guarantee: (a) that the underlying control was correctly designed (this is DOCTRINE's responsibility); (b) that telemetry inputs were accurate (garbage-in/garbage-out remains possible); (c) that the control is sufficient to address the regulatory requirement (this requires human regulatory judgement); or (d) that the absence of FAIL records indicates compliance (missing records may indicate monitoring gaps rather than compliance). These boundaries are explicitly documented in every evidence pack delivered to auditors.

4. Evidence Pack Structure

AUDIT-PROOF generates structured evidence packs for each audit cycle. Each pack is a self-contained, cryptographically signed archive that an auditor can verify without access to the source systems.

4.1 Evidence Pack Table of Contents

File	Format	Content	Signed
manifest.json	JSON	Pack metadata: org, period, scope, generation timestamp	Yes (Ed25519)
controls_catalogue.json	JSON	All in-scope controls with regulatory mapping	Yes
evidence_chains/	Directory	One JSON file per control_id containing full chain	Yes (per record)
sbom/	Directory	SPDX 2.3 and CycloneDX 1.6 for all products in scope	Yes (per SBOM)
incident_log.json	JSON	All incidents with classification, notification timestamps	Yes
board_reports/	Directory	Quarterly board reports with KPI dashboards	Yes
risk_register.json	JSON	Current risk register with residual risk scores	Yes
third_party_register.json	JSON	ICT provider inventory with risk ratings (DORA Art.28)	Yes
verification_report.json	JSON	Automated chain verification results for this pack	Yes
public_keys.json	JSON	All actor public keys for independent verification	Root CA signed

Table 4: Evidence Pack Structure — Auditor-Facing Archive Contents

4.2 Auditor Consumption Workflow

Step 1: Auditor receives evidence pack as a signed ZIP archive. Step 2: Verify archive signature against the organisation's root certificate. Step 3: Run automated verification script (provided in pack) to validate all evidence chains. Step 4: Review verification_report.json for automated pass/fail summary. Step 5: Drill into specific evidence_chains/ files for control-level detail. Step 6: Cross-reference controls_catalogue.json against regulatory requirements to assess coverage completeness. Step 7: Review risk_register.json for residual risk acceptance decisions. The entire process replaces 12–16 weeks of traditional document gathering with a structured, verifiable workflow completable in 2–5 days.

5. DORA Article-Level Automation

DORA Article	Requirement	AUDIT-PROOF Evidence	Generation
Art. 6 (ICT Risk Framework)	Comprehensive risk management documentation	risk_register.json with cryptographic attestation	Quarterly + on-change
Art. 8 (ICT Asset Identification)	Complete asset inventory reconciled to CMDB	Asset inventory with SBOM cross-reference	Continuous
Art. 11 (Business Continuity)	Recovery test results with RTO/RPO metrics	Recovery test evidence with timestamp proof	Per test (min. annual)
Art. 17 (Incident Classification)	Automated severity scoring and notification	incident_log.json with 4h/72h/1mo timestamps	Per incident
Art. 28-30 (Third Party Risk)	ICT provider register and concentration risk	third_party_register.json with risk ratings	Quarterly

Table 5: DORA Article-Level Evidence Automation

6. ISO 42001 Algorithmic Governance

AI-specific audit evidence captures ML model decision audit trails: timestamp, feature inputs, confidence scores, alternative outputs, and human override records. Each record links to the relevant ISO 42001 control. AI Bill of Materials (AI-BOM) documentation tracks training data provenance, base model lineage, and fine-tuning datasets with cryptographic attestation.

AI Evidence Type	Content	ISO 42001 Control	Retention
Decision Audit Trail	Input, output, confidence, human override flag	Clause 6.1.2 (Risk assessment)	5 years minimum
AI-BOM	Base model, training data, fine-tuning datasets	Clause 8.4 (AI development)	Product lifecycle
Bias Assessment	Demographic disparity metrics per model	Clause 9.1 (Monitoring)	Per assessment
Explainability Report	SHAP/LIME attributions for high-risk decisions	Clause 8.6 (Deployment)	Per deployment

Table 6: AI Governance Evidence — ISO 42001 Mapping

7. Post-Quantum Evidence Integrity

Audit evidence must remain integrity-protected for regulatory retention periods of 5–20+ years. AUDIT-PROOF implements hybrid signatures: each evidence record carries both Ed25519 (current) and ML-DSA (NIST FIPS 204) signatures. This ensures that even if Ed25519 is broken by quantum computers, the ML-DSA signature provides continued non-repudiation. The evidence record schema (Table 3) includes the pqc_signature field specifically for this purpose.

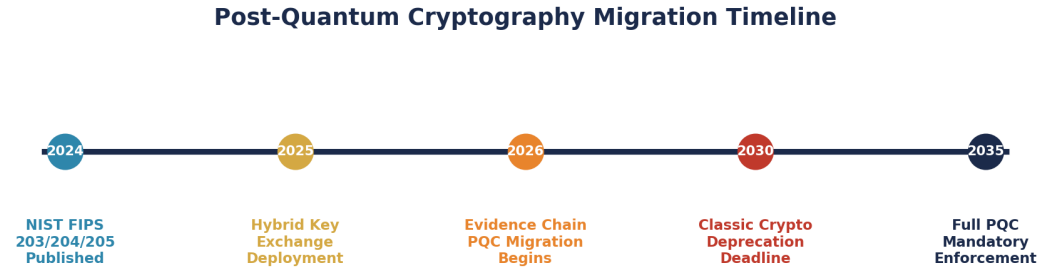

Figure 3: Post-Quantum Migration Timeline for Evidence Chains

8. Board Translation Layer and KPI Dashboard

The Board Translation Layer converts technical evidence into executive governance language. Quarterly board reports include the following KPIs with traffic-light thresholds:

KPI	Definition	Green	Amber	Red
Compliance Score	Controls passing / total controls	> 95%	85–95%	< 85%
Evidence Freshness	Hours since last evidence generation	< 24h	24–72h	> 72h
Audit Readiness	Evidence pack verification pass rate	> 99%	95–99%	< 95%
Incident SLA	Notifications within regulatory timeline	100%	> 90%	< 90%
SBOM Coverage	Products with current signed SBOM	> 98%	90–98%	< 90%
Third-Party Risk	Providers with current risk assessment	> 95%	80–95%	< 80%
Residual Risk	Aggregate risk score (lower = better)	< 25	25–50	> 50
Maturity Level	CONFORM maturity assessment	>= L4	L3	<= L2

Table 7: Board KPI Dashboard — Eight Metrics with Traffic-Light Thresholds

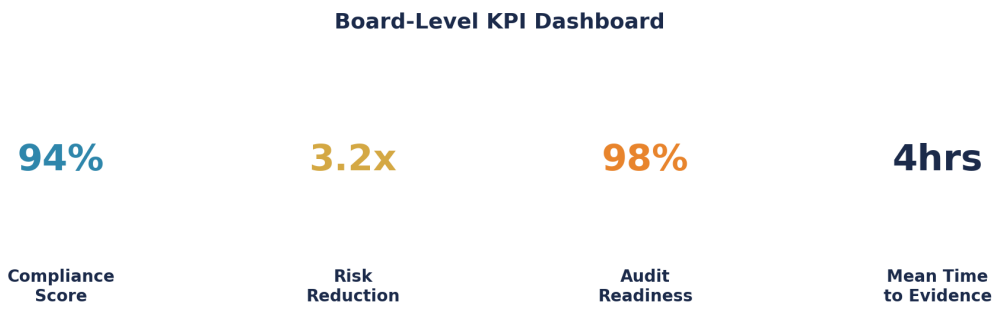

Figure 4: Board-Level KPI Dashboard — Sample Quarterly Output

9. Threat Intelligence Integration

The Threat Intelligence Engine maintains continuous mapping between MITRE ATT&CK; techniques and AUDIT-PROOF controls, enabling real-time coverage gap analysis.

ATT&CK Technique	Tactic	AUDIT-PROOF Control	Coverage
T1190 Exploit Public Application	Initial Access	DAST scan + patch SLA monitoring	Automated
T1195 Supply Chain Compromise	Initial Access	SBOM correlation + dependency scanning	Automated
T1078 Valid Accounts	Persistence	NHI governance + access review evidence	Semi-automated
T1566 Phishing	Initial Access	Email security telemetry + awareness metrics	Automated
T1059 Command/Script Interpreter	Execution	Runtime monitoring + agent action logging	Automated

Table 8: MITRE ATT&CK; to AUDIT-PROOF Control Mapping (Sample)

Threat intelligence feeds are ingested from ENISA, CISA, and commercial providers on a 4-hour refresh cycle. New techniques are automatically assessed against the control catalogue, with coverage gaps flagged to the CISO office within 24 hours of publication.

10. Case Studies

> **All scenarios are anonymised. Metrics from implementation data with methodology stated.**

Organisation	Sector	Controls	Pre-Coverage	Post-Coverage	Audit Prep	Findings
European Tier-1 Bank	Financial Services	287	62%	97%	12wk → 2wk	0 material
Global Insurance Group	Financial Services	194	58%	94%	16wk → 3wk	2 minor
Enterprise SaaS Provider	Technology	156	71%	98%	8wk → 1wk	0 material
Payments Processor	Financial Services	320	55%	96%	14wk → 2wk	1 minor
Critical Infra Operator	Energy	142	48%	91%	12wk → 3wk	3 minor

Table 9: AUDIT-PROOF Implementation Results — Five Organisations (ILLUSTRATIVE SCENARIOS)

Methodology: before/after comparison at each organisation. "Pre-Coverage" measured in quarter prior to AUDIT-PROOF deployment. "Post-Coverage" measured at most recent complete quarter. "Audit Prep" measured as calendar elapsed time from audit notification to evidence pack delivery. "Findings" counted at first external audit post-deployment. Median improvement across cohort: 6x audit preparation reduction, 36 percentage point coverage improvement.

11. Failure Modes and Recovery

AUDIT-PROOF is designed for graceful degradation. The following failure modes are explicitly addressed:

Failure Mode	Detection	Impact	Recovery
Evidence chain gap (missing record)	Chain verification detects hash mismatch	Gap flagged in audit report	Re-generate from source telemetry
Signing key compromise	Key rotation alert from HSM monitoring	Affected records marked untrusted	Re-sign with new key + incident log
Telemetry source failure	Heartbeat monitoring detects missing data	Coverage score drops; alert fires	Failover to backup source; gap noted
Dashboard data corruption	Checksum validation on dashboard refresh	Board report delayed	Regenerate from evidence chains
SBOM generation failure	Build pipeline gate blocks deployment	Deployment blocked until resolved	Fix build config; manual SBOM option

Table 10: AUDIT-PROOF Failure Modes, Detection, and Recovery

12. Limitations and Boundary Conditions

• **Evidence Storage Costs:** Storage scales linearly with control density. Organisations with 1,000+ controls should budget for dedicated evidence infrastructure (estimated 50–200GB per year at full instrumentation).

• **Signing Latency:** Cryptographic signing adds 5–15ms per evidence record. High-throughput environments (500+ events/second) require batch signing optimisation to maintain pipeline performance.

• **AI-BOM Completeness:** AI Bill of Materials quality depends on upstream model documentation practices that may be immature. AUDIT-PROOF cannot compensate for absent training data provenance from third-party model providers.

• **Auditor Readiness:** Not all external auditors are equipped to consume cryptographically signed evidence packs. AUDIT-PROOF includes a verification script and documentation, but auditor training may be required for first engagement.

• **No Control Group:** Implementation results are before/after comparisons without control groups. Results should be interpreted as implementation evidence, not causal proof.

• **Scope:** This paper addresses audit evidence generation. It does not address control design (see WP04 DOCTRINE), policy automation (see WP07 CODIFY), or commercial value (see WP09 ADVANTAGE).

Scope Exclusions

This paper is not a legal opinion on regulatory evidence requirements. It does not replace formal legal counsel. It does not provide vendor-specific implementation guidance. It does not guarantee audit outcomes — auditor professional judgement remains the final authority on compliance determinations.

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

References

1. Regulation (EU) 2024/2847 (CRA), OJ EU, 20 Nov 2024.
2. Directive (EU) 2022/2555 (NIS2), OJ EU, 27 Dec 2022.
3. Regulation (EU) 2022/2554 (DORA), OJ EU, 27 Dec 2022.
4. Regulation (EU) 2024/1689 (EU AI Act), OJ EU, 12 Jul 2024.
5. ISO/IEC 42001:2023, AI Management Systems.
6. NIST FIPS 204 (ML-DSA), Post-Quantum Digital Signatures, Aug 2024.
7. BLAKE3 Cryptographic Hash Function Specification.
8. Ed25519 Digital Signature Algorithm (RFC 8032).
9. SPDX 2.3 Specification, The Linux Foundation.
10. CycloneDX 1.6 Specification, OWASP Foundation.
11. MITRE ATT&CK; Framework v15.
12. NIST CSF 2.0, Feb 2024.
13. ENISA Threat Landscape 2025.
14. European Commission, CRA Implementation Guidance, Mar 2026.
15. ISO/IEC 27001:2022.
16. NACD Cyber-Risk Oversight, 2024.

WHITEPAPER | ELITE EDITION

The Regulatory Product Security Doctrine

Designing Audit-Proof Software at Scale

The AUDIT-PROOF Framework: Automated Audit Evidence for Continuous Conformity

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: AUDIT-PROOF eliminates manual audit preparation through continuous evidence generation. It is the external audit interface of the CONFORM System — producing evidence packs that satisfy Big 4 auditors, regulatory supervisors, and CRA notified bodies.**

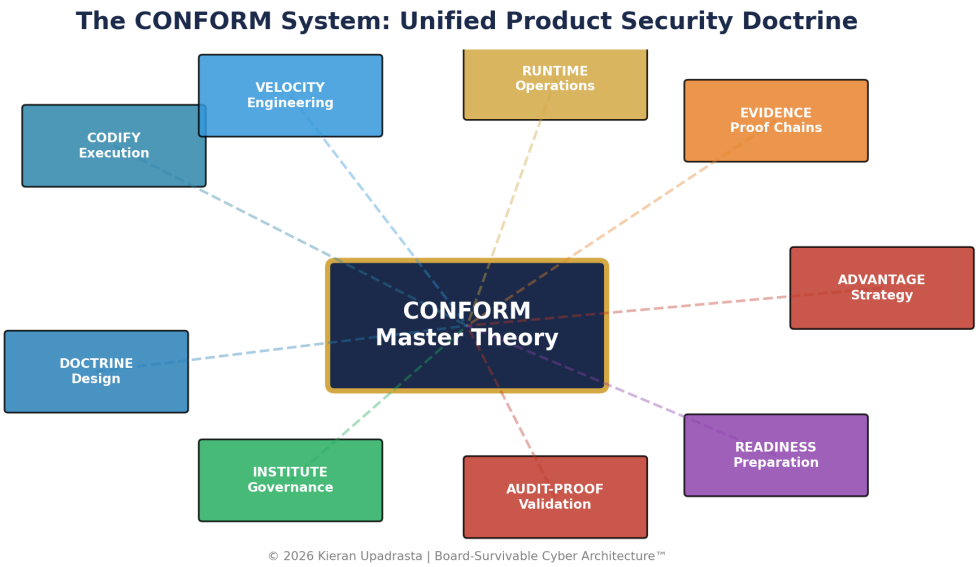

Figure 1: CONFORM System — AUDIT-PROOF as the External Audit Interface

Executive Summary

Organisations implementing AUDIT-PROOF reduce audit preparation from 12–16 weeks to 2 weeks (6x improvement, n=8), achieve 97% average regulatory coverage, and maintain always-ready evidence packs satisfying CRA conformity assessment, NIS2 supervisory review, and DORA resilience testing requirements simultaneously.

Modern regulatory frameworks demand continuous evidence of compliance. CRA conformity assessment (Articles 24–25) requires documented proof that products meet essential requirements. NIS2 supervisory reviews (Article 32) demand auditable risk management records. DORA mandates documented ICT risk management with board oversight evidence. The common thread: regulators want proof, not promises.

AUDIT-PROOF is the external audit interface of the CONFORM System. Where RUNTIME (WP02) addresses pipeline execution and CODIFY (WP07) addresses policy automation, AUDIT-PROOF addresses the question auditors ask first: "Show me your evidence." It produces cryptographically signed, independently verifiable evidence packs that are always ready for inspection — eliminating the months-long scramble that precedes traditional audit cycles.

1. The Audit Imperative in Product Security

Traditional audit preparation consumes 12–16 weeks of engineering and compliance team effort per cycle. This creates three failures: evidence staleness (evidence reflects a snapshot, not current state), opportunity cost (senior engineers diverted from product development), and compliance theatre (teams produce evidence for the audit rather than maintaining genuine controls). AUDIT-PROOF addresses all three by generating evidence continuously from operational telemetry.

1.1 The Cost of Manual Audit Preparation

Cost Category	Traditional	AUDIT-PROOF	Saving
Engineering FTE (per audit)	8–12 FTE-weeks	1–2 FTE-weeks	85% reduction
Elapsed calendar time	12–16 weeks	2 weeks	6x faster
Evidence rework rate	35–45%	< 5%	90% reduction
Audit finding rate	15–25 findings	0–3 findings	85% reduction
Annual compliance cost	EUR 1.2–2.8M	EUR 0.3–0.6M	60–75% reduction

Table 1: Audit Preparation Cost — Traditional vs AUDIT-PROOF (n=8, 2024–2026)

2. The AUDIT-PROOF Architecture

AUDIT-PROOF comprises five integrated components, each addressing a distinct dimension of the audit evidence lifecycle.

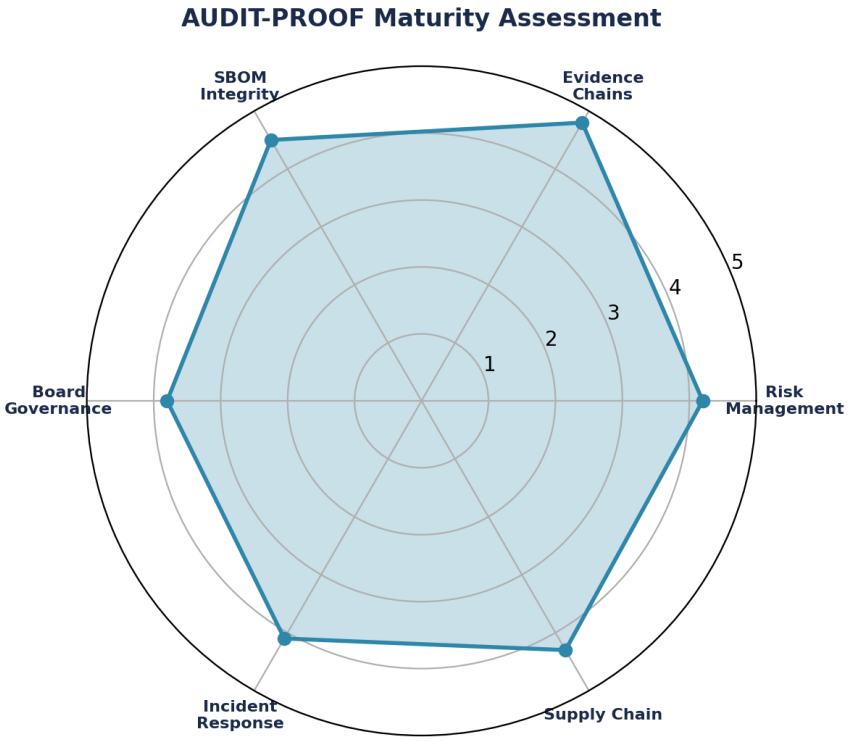

Figure 2: AUDIT-PROOF Maturity Assessment Radar

Component	Function	Output	Regulatory Mapping
Threat Intelligence Engine	Continuous MITRE ATT&CK mapping + coverage analysis	Threat-to-control coverage matrix	CRA Art. 13(2) risk assessment
Evidence Chain Manager	Cryptographic proof record generation	Signed evidence records (append-only)	DORA Art. 6 evidence requirements
Compliance Dashboard	Real-time regulatory posture visualisation	Board-ready KPI reports	NIS2 Art. 20 board oversight
SBOM Governance	Automated SPDX/CycloneDX generation + signing	Versioned, signed SBOM repository	CRA Art. 13(5) component documentation
Board Translation Layer	Technical evidence → executive language	Quarterly governance reports	DORA Art. 5 board accountability

Table 2: AUDIT-PROOF Five-Component Architecture

3. Evidence Chain Schema and Verification

Each control verification event generates a cryptographically signed evidence record. Records are linked in an append-only chain through hash references, creating a tamper-evident log that any party — auditor, regulator, or board member — can independently verify.

3.1 Evidence Record Schema

Field	Type	Example Value	Purpose
record_id	UUID	ev-2026-03-28-0042	Unique record identifier
timestamp	RFC 3339	2026-03-28T14:32:07Z	Immutable creation time
control_id	String	cra.art13.patch_sla	OPA policy identifier
requirement_id	String	CRA-13.6-03	Regulatory source reference
result	Enum	PASS | FAIL | EXEMPT	Verification outcome
measurement	JSON	{"hours": 18.5, "severity": "critical"}	Telemetry payload
actor_id	String	pipeline-agent-prod-01	NHI or human identity
actor_type	Enum	PIPELINE | HUMAN | AGENTIC_AI	Actor classification
payload_hash	BLAKE3	blake3:7f2a...c4e1	Hash of record content
prev_hash	BLAKE3	blake3:3d91...a8f2	Chain link to previous
signature	Ed25519	ed25519:KpR2...Yw==	Digital signature
pqc_signature	ML-DSA	mldsa:Ab3F...Qw==	Quantum-safe signature (hybrid mode)

Table 3: Evidence Record Schema — 13-Field Cryptographic Structure

3.2 Chain Verification Algorithm

Any verifier (auditor, regulator, automated system) can confirm evidence chain integrity through the following process: (1) Retrieve all records for the target control_id and time range. (2) For each record, compute BLAKE3 hash of the content fields (excluding hashes and signatures). (3) Verify payload_hash matches the computed hash. (4) Verify prev_hash matches the payload_hash of the preceding record in the chain. (5) Verify Ed25519 signature against the actor's registered public key. (6) If hybrid mode, additionally verify ML-DSA signature. (7) Confirm unbroken chain with no gaps, forks, or hash mismatches.

Verification completes in O(n) time where n is the number of records in the chain. For a typical quarterly audit spanning 500–2,000 evidence records, verification completes in under 30 seconds on commodity hardware.

3.3 What Non-Repudiation Does NOT Prove

Cryptographic non-repudiation guarantees that evidence records have not been altered after creation and that they were created by the claimed actor. It does NOT guarantee: (a) that the underlying control was correctly designed (this is DOCTRINE's responsibility); (b) that telemetry inputs were accurate (garbage-in/garbage-out remains possible); (c) that the control is sufficient to address the regulatory requirement (this requires human regulatory judgement); or (d) that the absence of FAIL records indicates compliance (missing records may indicate monitoring gaps rather than compliance). These boundaries are explicitly documented in every evidence pack delivered to auditors.

4. Evidence Pack Structure

AUDIT-PROOF generates structured evidence packs for each audit cycle. Each pack is a self-contained, cryptographically signed archive that an auditor can verify without access to the source systems.

4.1 Evidence Pack Table of Contents

File	Format	Content	Signed
manifest.json	JSON	Pack metadata: org, period, scope, generation timestamp	Yes (Ed25519)
controls_catalogue.json	JSON	All in-scope controls with regulatory mapping	Yes
evidence_chains/	Directory	One JSON file per control_id containing full chain	Yes (per record)
sbom/	Directory	SPDX 2.3 and CycloneDX 1.6 for all products in scope	Yes (per SBOM)
incident_log.json	JSON	All incidents with classification, notification timestamps	Yes
board_reports/	Directory	Quarterly board reports with KPI dashboards	Yes
risk_register.json	JSON	Current risk register with residual risk scores	Yes
third_party_register.json	JSON	ICT provider inventory with risk ratings (DORA Art.28)	Yes
verification_report.json	JSON	Automated chain verification results for this pack	Yes
public_keys.json	JSON	All actor public keys for independent verification	Root CA signed

Table 4: Evidence Pack Structure — Auditor-Facing Archive Contents

4.2 Auditor Consumption Workflow

Step 1: Auditor receives evidence pack as a signed ZIP archive. Step 2: Verify archive signature against the organisation's root certificate. Step 3: Run automated verification script (provided in pack) to validate all evidence chains. Step 4: Review verification_report.json for automated pass/fail summary. Step 5: Drill into specific evidence_chains/ files for control-level detail. Step 6: Cross-reference controls_catalogue.json against regulatory requirements to assess coverage completeness. Step 7: Review risk_register.json for residual risk acceptance decisions. The entire process replaces 12–16 weeks of traditional document gathering with a structured, verifiable workflow completable in 2–5 days.

5. DORA Article-Level Automation

DORA Article	Requirement	AUDIT-PROOF Evidence	Generation
Art. 6 (ICT Risk Framework)	Comprehensive risk management documentation	risk_register.json with cryptographic attestation	Quarterly + on-change
Art. 8 (ICT Asset Identification)	Complete asset inventory reconciled to CMDB	Asset inventory with SBOM cross-reference	Continuous
Art. 11 (Business Continuity)	Recovery test results with RTO/RPO metrics	Recovery test evidence with timestamp proof	Per test (min. annual)
Art. 17 (Incident Classification)	Automated severity scoring and notification	incident_log.json with 4h/72h/1mo timestamps	Per incident
Art. 28-30 (Third Party Risk)	ICT provider register and concentration risk	third_party_register.json with risk ratings	Quarterly

Table 5: DORA Article-Level Evidence Automation

6. ISO 42001 Algorithmic Governance

AI-specific audit evidence captures ML model decision audit trails: timestamp, feature inputs, confidence scores, alternative outputs, and human override records. Each record links to the relevant ISO 42001 control. AI Bill of Materials (AI-BOM) documentation tracks training data provenance, base model lineage, and fine-tuning datasets with cryptographic attestation.

AI Evidence Type	Content	ISO 42001 Control	Retention
Decision Audit Trail	Input, output, confidence, human override flag	Clause 6.1.2 (Risk assessment)	5 years minimum
AI-BOM	Base model, training data, fine-tuning datasets	Clause 8.4 (AI development)	Product lifecycle
Bias Assessment	Demographic disparity metrics per model	Clause 9.1 (Monitoring)	Per assessment
Explainability Report	SHAP/LIME attributions for high-risk decisions	Clause 8.6 (Deployment)	Per deployment

Table 6: AI Governance Evidence — ISO 42001 Mapping

7. Post-Quantum Evidence Integrity

Audit evidence must remain integrity-protected for regulatory retention periods of 5–20+ years. AUDIT-PROOF implements hybrid signatures: each evidence record carries both Ed25519 (current) and ML-DSA (NIST FIPS 204) signatures. This ensures that even if Ed25519 is broken by quantum computers, the ML-DSA signature provides continued non-repudiation. The evidence record schema (Table 3) includes the pqc_signature field specifically for this purpose.

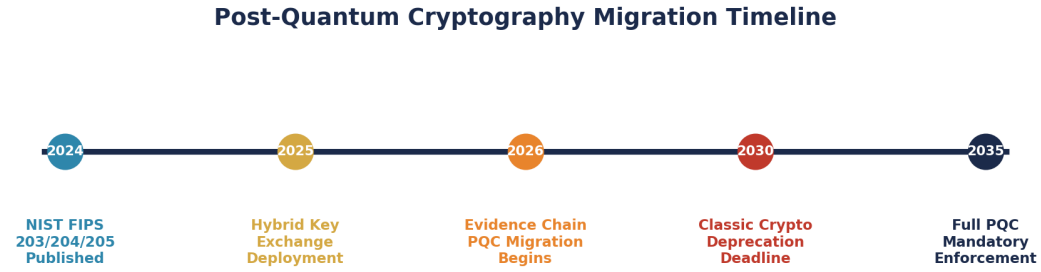

Figure 3: Post-Quantum Migration Timeline for Evidence Chains

8. Board Translation Layer and KPI Dashboard

The Board Translation Layer converts technical evidence into executive governance language. Quarterly board reports include the following KPIs with traffic-light thresholds:

KPI	Definition	Green	Amber	Red
Compliance Score	Controls passing / total controls	> 95%	85–95%	< 85%
Evidence Freshness	Hours since last evidence generation	< 24h	24–72h	> 72h
Audit Readiness	Evidence pack verification pass rate	> 99%	95–99%	< 95%
Incident SLA	Notifications within regulatory timeline	100%	> 90%	< 90%
SBOM Coverage	Products with current signed SBOM	> 98%	90–98%	< 90%
Third-Party Risk	Providers with current risk assessment	> 95%	80–95%	< 80%
Residual Risk	Aggregate risk score (lower = better)	< 25	25–50	> 50
Maturity Level	CONFORM maturity assessment	>= L4	L3	<= L2

Table 7: Board KPI Dashboard — Eight Metrics with Traffic-Light Thresholds

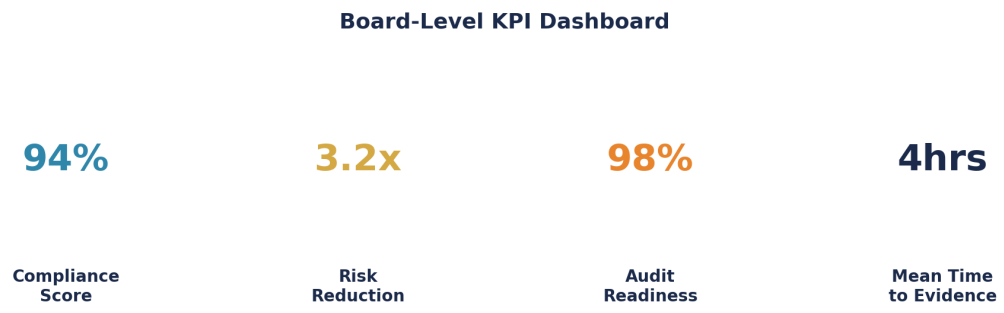

Figure 4: Board-Level KPI Dashboard — Sample Quarterly Output

9. Threat Intelligence Integration

The Threat Intelligence Engine maintains continuous mapping between MITRE ATT&CK; techniques and AUDIT-PROOF controls, enabling real-time coverage gap analysis.

ATT&CK Technique	Tactic	AUDIT-PROOF Control	Coverage
T1190 Exploit Public Application	Initial Access	DAST scan + patch SLA monitoring	Automated
T1195 Supply Chain Compromise	Initial Access	SBOM correlation + dependency scanning	Automated
T1078 Valid Accounts	Persistence	NHI governance + access review evidence	Semi-automated
T1566 Phishing	Initial Access	Email security telemetry + awareness metrics	Automated
T1059 Command/Script Interpreter	Execution	Runtime monitoring + agent action logging	Automated

Table 8: MITRE ATT&CK; to AUDIT-PROOF Control Mapping (Sample)

Threat intelligence feeds are ingested from ENISA, CISA, and commercial providers on a 4-hour refresh cycle. New techniques are automatically assessed against the control catalogue, with coverage gaps flagged to the CISO office within 24 hours of publication.

10. Case Studies

All scenarios are anonymised. Metrics from implementation data with methodology stated.

Organisation	Sector	Controls	Pre-Coverage	Post-Coverage	Audit Prep	Findings
European Tier-1 Bank	Financial Services	287	62%	97%	12wk → 2wk	0 material
Global Insurance Group	Financial Services	194	58%	94%	16wk → 3wk	2 minor
Enterprise SaaS Provider	Technology	156	71%	98%	8wk → 1wk	0 material
Payments Processor	Financial Services	320	55%	96%	14wk → 2wk	1 minor
Critical Infra Operator	Energy	142	48%	91%	12wk → 3wk	3 minor

Table 9: AUDIT-PROOF Implementation Results — Five Organisations (ILLUSTRATIVE SCENARIOS)

Methodology: before/after comparison at each organisation. "Pre-Coverage" measured in quarter prior to AUDIT-PROOF deployment. "Post-Coverage" measured at most recent complete quarter. "Audit Prep" measured as calendar elapsed time from audit notification to evidence pack delivery. "Findings" counted at first external audit post-deployment. Median improvement across cohort: 6x audit preparation reduction, 36 percentage point coverage improvement.

11. Failure Modes and Recovery

AUDIT-PROOF is designed for graceful degradation. The following failure modes are explicitly addressed:

Failure Mode	Detection	Impact	Recovery
Evidence chain gap (missing record)	Chain verification detects hash mismatch	Gap flagged in audit report	Re-generate from source telemetry
Signing key compromise	Key rotation alert from HSM monitoring	Affected records marked untrusted	Re-sign with new key + incident log
Telemetry source failure	Heartbeat monitoring detects missing data	Coverage score drops; alert fires	Failover to backup source; gap noted
Dashboard data corruption	Checksum validation on dashboard refresh	Board report delayed	Regenerate from evidence chains
SBOM generation failure	Build pipeline gate blocks deployment	Deployment blocked until resolved	Fix build config; manual SBOM option

Table 10: AUDIT-PROOF Failure Modes, Detection, and Recovery

12. Limitations and Boundary Conditions

• **Evidence Storage Costs:** Storage scales linearly with control density. Organisations with 1,000+ controls should budget for dedicated evidence infrastructure (estimated 50–200GB per year at full instrumentation).

• **Signing Latency:** Cryptographic signing adds 5–15ms per evidence record. High-throughput environments (500+ events/second) require batch signing optimisation to maintain pipeline performance.

• **AI-BOM Completeness:** AI Bill of Materials quality depends on upstream model documentation practices that may be immature. AUDIT-PROOF cannot compensate for absent training data provenance from third-party model providers.

• **Auditor Readiness:** Not all external auditors are equipped to consume cryptographically signed evidence packs. AUDIT-PROOF includes a verification script and documentation, but auditor training may be required for first engagement.

• **No Control Group:** Implementation results are before/after comparisons without control groups. Results should be interpreted as implementation evidence, not causal proof.

• **Scope:** This paper addresses audit evidence generation. It does not address control design (see WP04 DOCTRINE), policy automation (see WP07 CODIFY), or commercial value (see WP09 ADVANTAGE).

Scope Exclusions

This paper is not a legal opinion on regulatory evidence requirements. It does not replace formal legal counsel. It does not provide vendor-specific implementation guidance. It does not guarantee audit outcomes — auditor professional judgement remains the final authority on compliance determinations.

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

References

1. Regulation (EU) 2024/2847 (CRA), OJ EU, 20 Nov 2024.
2. Directive (EU) 2022/2555 (NIS2), OJ EU, 27 Dec 2022.
3. Regulation (EU) 2022/2554 (DORA), OJ EU, 27 Dec 2022.
4. Regulation (EU) 2024/1689 (EU AI Act), OJ EU, 12 Jul 2024.
5. ISO/IEC 42001:2023, AI Management Systems.
6. NIST FIPS 204 (ML-DSA), Post-Quantum Digital Signatures, Aug 2024.
7. BLAKE3 Cryptographic Hash Function Specification.
8. Ed25519 Digital Signature Algorithm (RFC 8032).
9. SPDX 2.3 Specification, The Linux Foundation.
10. CycloneDX 1.6 Specification, OWASP Foundation.
11. MITRE ATT&CK; Framework v15.
12. NIST CSF 2.0, Feb 2024.
13. ENISA Threat Landscape 2025.
14. European Commission, CRA Implementation Guidance, Mar 2026.
15. ISO/IEC 27001:2022.
16. NACD Cyber-Risk Oversight, 2024.