AffixIO Technical Paper · WP-007
June 2026
affix-io.com

AFFIXIO WHITE PAPER · WP-007

Building for the EU AI Act and NIS2 Simultaneously: One Architecture, Dual Compliance

Stop building two audit stacks for one AI platform.

AffixIO | United Kingdom | affix-io.com | June 2026

ABSTRACT

AI Act and NIS2 overlap but land on different teams. AffixIO's proof pipeline satisfies documentation, logging, transparency, and security monitoring in one pass, so legal and SecOps stop duplicating evidence collection.

CONTENTS

1 Introduction
2 Regulatory Overview
3 Mapping to EU AI Act Articles
4 Mapping to NIS2 Security Measures

5 Shared Infrastructure: Where One Implementation Satisfies Both
6 AI Act Specific Requirements
7 NIS2 Specific Requirements
8 Dual Compliance Architecture Diagram
9 Incident Reporting Integration
10 Supply Chain Assurance
11 Known Gaps and Remaining Work
12 Conclusion

SECTION 1

Introduction

Regulated AI deployment in Europe in 2026 requires simultaneous attention to two frameworks that were developed independently, are administered by different regulatory bodies, and use different vocabularies for overlapping concepts. The EU AI Act is administered by national market surveillance authorities and the European AI Office; NIS2 is administered by national cybersecurity agencies and CERTs. The AI Act focuses on AI system quality, transparency, and risk management; NIS2 focuses on cybersecurity resilience, incident response, and supply chain security. Yet both frameworks create requirements that apply to the same infrastructure: AI systems deployed by essential and important entities under NIS2, which are also high-risk AI systems under the AI Act.

The natural response to dual regulation is to build dual compliance programmes: one team addresses AI Act requirements, another addresses NIS2 requirements, and the programmes are coordinated at a governance level. This approach is costly and creates complexity at the boundary between the two programmes. AffixIO's architecture suggests a different approach: build infrastructure that is structurally aligned with both frameworks' requirements, so that a single implementation generates compliance artefacts for both programmes simultaneously.

This is possible because the core technical requirements of both frameworks, audit trails, tamper-evidence, documentation integrity, cybersecurity measures, and supply chain assurance, are all satisfied by cryptographic governance infrastructure. A ZK proof anchored in a Merkle tree and signed with post-quantum keys is both an AI Act audit record and a NIS2 security measure, depending on how it is characterised in the compliance programme.

SECTION 2

Regulatory Overview

The EU AI Act establishes risk categories for AI systems and imposes obligations on providers of high-risk AI systems. Articles 11-17 set out the technical and quality management requirements for high-risk AI system providers: technical documentation (Article 11), record-keeping (Article 12), transparency (Article 13), human oversight (Article 14), accuracy and robustness (Article 15), quality management systems (Article 17), and conformity assessment (Article 43). These requirements were applicable to high-risk AI systems from August 2026.

NIS2 requires essential and important entities to implement appropriate technical and organisational security measures, including risk management policies, incident handling, business continuity, supply chain security, network security, and cryptographic policies. Article 21 of NIS2 specifies minimum security measures including the use of cryptography and encryption where appropriate. Annex I identifies sectors to which NIS2 applies, including digital infrastructure, digital services, and public administration, all of which may deploy regulated AI systems.

The intersection is significant. An entity that provides digital services (NIS2 essential or important entity) and deploys an AI system that makes decisions affecting service quality or user eligibility (potentially high-risk AI under the AI Act) is subject to both frameworks for the same infrastructure. The compliance question is whether a single technical implementation can satisfy both.

SECTION 3

Mapping to EU AI Act Articles

AI ACT ARTICLE	REQUIREMENT	AFFIXIO IMPLEMENTATION	EVIDENCE
Art. 11 (Technical documentation)	Maintain technical documentation throughout system lifecycle	Immutable ZK proof audit trail with signed Merkle roots	Proof digest + signed root per response
Art. 12 (Record-keeping)	Automatic logging capability for relevant data	compliance record service with append-only proof records	Proof count with timestamps
Art. 13 (Transparency)	Inform users of AI system status	Verification disclosure on every response	Badge with circuit id and outcome
Art. 14 (Human oversight)	Enable human intervention where necessary	NO outcome triggers human review queue	Alert on citation_signal = 0 or circuit NO
Art. 15 (Accuracy and robustness)	Appropriate cybersecurity measures	ML-DSA-65 post-quantum signing + HSM key custody	FIPS 140-2 L3 HSM attestation certificate
Art. 17 (Quality management)	Systematic quality management system	Automated proof generation for every response	Proof coverage rate metric

The technical documentation requirement in Article 11 is particularly well served by the ZK proof audit trail. Conventional technical documentation is a static set of documents maintained alongside the AI system. The ZK proof audit trail is dynamic documentation: it grows with every AI response and provides a timestamped, cryptographically verifiable record of every governance decision made by the system. This is a stronger form of technical documentation than the conventional approach, because it is continuously updated and tamper-resistant.

SECTION 4

Mapping to NIS2 Security Measures

NIS2 MEASURE	REQUIREMENT	AFFIXIO IMPLEMENTATION
Risk management policies	Policies addressing risks to network and information systems	ZK circuit encodes machine-readable policy; policy version in proof
Incident handling	Incident detection, response, and recovery procedures	NO outcome audit trail; anomaly detection on proof rate
Supply chain security	Security measures relating to the security of supply chain	Open-source, auditable components (constraint language MIT, proving backend MIT)
Network and information systems security	Policies and procedures to assess security measures effectiveness	Merkle root integrity verifiable independently of AffixIO
Cryptographic policies	Use of cryptography and encryption where appropriate	ML-DSA-65 (NIST FIPS 204), SHA-256, BN254 elliptic curve
Access control and asset management	Control access to network and information systems	HSM key custody; circuit artefacts under version control

The NIS2 cryptographic policies measure is directly satisfied by AffixIO's post-quantum signing infrastructure. NIS2 Article 21(2)(h) requires that entities implement "policies and procedures regarding the use of cryptography and, where appropriate, encryption." The ML-DSA-65 / SHA-256 / BN254 stack satisfies this requirement with specific algorithmic choices traceable to NIST and IETF standards.

SECTION 5

Shared Infrastructure: Where One Implementation Satisfies Both

Five components of AffixIO's production architecture generate compliance artefacts that simultaneously satisfy AI Act and NIS2 requirements.

The ZK proof audit trail satisfies AI Act Article 11 (technical documentation) and NIS2 incident handling. The same cryptographically verifiable record of every AI governance decision is both the technical documentation and the incident evidence base.

The Merkle tree and signed roots log satisfies AI Act Article 12 (record-keeping) and NIS2 network and information systems security. The independently verifiable completeness of the Merkle tree satisfies record-keeping requirements without depending on the operator's trustworthiness.

The ML-DSA-65 post-quantum signing satisfies AI Act Article 15 (cybersecurity measures) and NIS2 cryptographic policies. A single key management and signing infrastructure satisfies both frameworks' cryptographic requirements.

The verification disclosure satisfies AI Act Article 13 (transparency to users) and NIS2 incident handling (users notified when a response fails governance). The badge provides both transparency information for the AI Act and notification functionality for NIS2.

The open-source circuit library satisfies AI Act Article 17 (quality management) and NIS2 supply chain security. Open-source components under MIT and Apache licences are auditable by any party, satisfying supply chain security requirements without vendor-specific assurance documentation.

SECTION 6

AI Act Specific Requirements

Three AI Act requirements have no direct NIS2 counterpart and require AI-Act-specific implementation.

Article 14 (human oversight) requires that high-risk AI systems enable natural persons to oversee the AI system's functioning and intervene where necessary. AffixIO's governance architecture generates evidence for human oversight decisions but does not itself implement the oversight workflow. Organisations deploying AffixIO governance must implement a human review queue that receives NO-outcome alerts and a process for reviewing and acting on those alerts. This is an organisational requirement that the cryptographic governance infrastructure supports but cannot fulfil alone.

Article 43 (conformity assessment) requires that certain high-risk AI systems undergo third-party conformity assessment before being placed on the market. The ZK proof audit trail can support a conformity assessment by providing verifiable evidence of governance operation, but the conformity assessment itself is a regulatory process that requires engagement with a notified body. AffixIO can generate the technical documentation required for the conformity assessment, but cannot substitute for the assessment process.

The registration obligation (Article 51) requires high-risk AI system providers to register their systems in the EU AI database before placing them on the market. This is an administrative requirement with no technical implementation component and is outside the scope of AffixIO's technical governance architecture.

SECTION 7

NIS2 Specific Requirements

Three NIS2 requirements have no direct AI Act counterpart and require NIS2-specific implementation.

Incident notification (Article 23) requires essential and important entities to notify the competent authority of significant incidents within 24 hours of becoming aware of them. AffixIO's governance architecture provides the evidence base for incident notifications (the proof audit trail shows what happened and when) but does not implement the notification process. Organisations subject to NIS2 must implement incident response procedures that use the governance trail as evidence and generate notifications in accordance with Article 23.

Business continuity (Article 21(2)(c)) requires that entities implement business continuity policies including backup management, disaster recovery, and crisis management. AffixIO's Merkle roots log provides verifiable continuity of the governance record, but backup and disaster recovery for the compliance record service and Merkle tree service are operational requirements that must be addressed separately.

Multi-factor authentication (Article 21(2)(j)) requires appropriate use of MFA for access to network and information systems. This is an access control requirement that applies to the AffixIO governance infrastructure administration and must be implemented at the infrastructure level.

SECTION 8

Dual Compliance Architecture

The following table summarises which architecture components provide compliance evidence for which frameworks, showing the dual-use nature of the shared infrastructure.

COMPONENT	EU AI ACT ARTICLES SATISFIED	NIS2 MEASURES SATISFIED
ZK proof generation	Art. 11, 12, 15, 17	Risk management, cryptographic policies
Merkle tree anchoring	Art. 11, 12	Network security, incident handling
ML-DSA-65 signing + HSM	Art. 15	Cryptographic policies, access control
Verification disclosure	Art. 13	Incident notification (user-facing)
Open-source circuit library	Art. 17	Supply chain security
compliance record service audit trail	Art. 11, 12	Incident handling, business continuity evidence

SECTION 9

Incident Reporting Integration

Both the AI Act and NIS2 require incident reporting capabilities. The ZK proof audit trail supports incident reporting by providing a cryptographically verifiable, timestamped record of every governance event. When an incident occurs (a governance failure, an anomalous pattern of NO outcomes, or a suspected compromise of the signing infrastructure), the audit trail provides the evidence base for the incident report.

For NIS2 Article 23 early warning notifications (within 24 hours of awareness), the audit trail timestamp provides the earliest possible evidence of when anomalous governance behaviour began, supporting accurate incident timing in notifications. For AI Act Article 73 serious incident reporting, the audit trail provides a complete record of governance decisions in the period surrounding the incident, including whether the relevant AI responses passed or failed governance checks.

SECTION 10

Supply Chain Assurance

Both frameworks create supply chain assurance requirements. The AI Act's Article 28 requires deployers to verify that providers of high-risk AI systems comply with the Act. NIS2's supply chain security measure requires entities to assess the security practices of their suppliers. AffixIO's open-source architecture addresses supply chain assurance directly: all cryptographic components (Noir, proving backend, the client interface layer, a federated retrieval component, a content extraction component, an application framework) are open-source, have publicly auditable licences, and have active security disclosure programmes.

The open-source supply chain is auditable in a way that proprietary components cannot be. A security researcher or compliance auditor can inspect the policy circuit compiler, the production proving system, and the the client interface layer interface code. The HSM (a certified HSM) is a proprietary component but is covered by AWS's FedRAMP and ISO 27001 certifications, providing independent assurance. The ML-DSA-65 algorithm is specified in NIST FIPS 204, a public standard that has undergone extensive public review.

SECTION 11

Known Gaps and Remaining Work

The dual compliance architecture described here addresses the technical infrastructure requirements of both frameworks. It does not address all compliance requirements. Organisations adopting this architecture should conduct their own gap analysis covering: the human oversight workflow required by AI Act Article 14, the conformity assessment process required by AI Act Article 43 for applicable systems, the incident notification procedures required by NIS2 Article 23, the business continuity programme required by NIS2 Article 21(2)(c), and the administrative registration requirements of the AI Act's Article 51 EU AI database.

Legal and regulatory advice is essential before relying on this architecture for compliance purposes. The regulatory landscape is evolving rapidly: the AI Act's implementing acts are being published on a rolling basis, and NIS2 transposition varies by member state. This whitepaper reflects the framework as understood in June 2026 and should be reviewed against current implementing measures before use in compliance planning.

SECTION 12

Conclusion

The EU AI Act and NIS2 Directive are not aligned by design, but their technical infrastructure requirements converge significantly at the intersection of AI systems and cybersecurity. A cryptographic governance architecture based on ZK proofs, Merkle anchoring, and post-quantum signatures simultaneously addresses the audit trail, documentation integrity, transparency, and cryptographic security requirements of both frameworks. The overlap is not coincidental: both frameworks respond to the same underlying problem of providing trustworthy evidence of what AI systems do and how they are secured.

Building dual compliance programmes for overlapping frameworks is expensive. Building a single cryptographic infrastructure that generates compliance artefacts for both is more efficient and produces stronger evidence, because the artefacts are mathematically verifiable rather than procedurally asserted. AffixIO's production architecture demonstrates that this is achievable today, not a future aspiration.

Related reading

- WP-020: DORA-Compliant AI Governance with Zero-Knowledge Audit Records
- WP-001: Cryptographic AI Governance: A Technical Framework

- WP-004: Real-Time Zero-Knowledge Governance in the AI Response Pipeline

Frequently asked questions

Can one system satisfy both frameworks?

Shared cryptographic records cover AI Act Articles 11 to 15 and NIS2 security monitoring evidence when mapped correctly.

What about NIS2 incident notification?

Proof failures integrate with SIEM workflows; Article 23 notification processes remain organisational responsibilities.

When did high-risk AI Act duties apply?

High-risk provider obligations under Articles 11 to 15 applied from August 2026 for in-scope systems.