Synchronicity – Standards Mapping Reference

One page. Eight standards. The technical control substrate behind each.

Synchronicity is an external governance authority for autonomous AI. Every proposed action is canonicalized as a structured descriptor, evaluated against versioned policy, and either PERMITted, DENYed, or HELD. Each decision produces a cryptographically signed, deterministically replayable artifact.

The table below shows how the architecture maps to the standards procurement, GRC, and audit teams actually ask about.

Standards Mapping

Standard	Specific reference	How Synchronicity maps
ISO/IEC 42001:2023	§8.2 AI system inventory	SPADs and actor metadata are the inventory substrate
	§8.5 Monitoring and measurement	Append-only signed decision log
	§6.1.2 Risk assessment	Policy versioning and content-hashed snapshots
	§6.1.3 Risk treatment	Fail-closed semantics, default-deny
	§8.4 AI system impact assessment	Model-identity tracking in SPADs
NIST AI RMF 1.0	Govern	Policy authoring and version control
	Map	Structured Proposed Action Descriptor (SPAD) ontology
	Measure	Append-only artifact log of all PERMIT, DENY, HOLD outcomes
	Manage	HOLD routing and termination authority
	Manage-2.2 / 4.1	Post-deployment monitoring of model changes
EU AI Act (Reg. 2024/1689)	Art. 9 Risk management	Policy layers and HOLD routing
	Art. 10 Data governance	Input lineage in SPADs

Standard	Specific reference	How Synchronicity maps
	Art. 11 Technical documentation	Self-documenting policy version manifest
	Art. 12 Logging	Signed, replayable decision artifacts
	Art. 13 Transparency	Cryptographic policy content hash recorded per decision
	Art. 14 Human oversight	HOLD outcomes and termination authority
	Art. 15 Accuracy, robustness, cybersecurity	Default-deny + signed authority
	Art. 40 Presumption of conformity	Architecture aligns to harmonized standards
	Art. 72 Post-market monitoring	Model-identity tracking, drift signal ingestion
	Art. 78 + Recital 71 Confidentiality	Compliance provable without disclosing policy content
OWASP AISVS	C2 User input validation	Action descriptors carry input lineage; untrusted inputs denied
	C3 Model lifecycle & change control	Policy versioning + signed snapshots for model behavior changes
	C4 Infrastructure & deployment	Authority is the deployed control plane; default-deny on failure
	C5 Access control & identity	Actor-to-capability binding; scope and privilege-escalation enforcement
	C5.6 / C5.6.5 / C5.6.6	Unauthorized actions, action chaining, authority hardening (founder contributor)
	C6 Supply chain	Policy rules require attested model and data provenance
	C7 Model behavior & output control	Every model-proposed action is gated by policy before execution
	C9 Autonomous orchestration	Core domain: agentic action authorization end-to-end
	C9.7 / C9.7.7	Tool/credential scope, prompt injection at action layer (founder contributor)

Standard	Specific reference	How Synchronicity maps
	C10 MCP security	MCP tool invocations are governed actions; identity verified per call
	C11 Adversarial robustness	Prompt injection contained at action layer; models cannot unilaterally execute
	C12 Privacy & personal data	Data-class policy enforcement; signed log of every data-touching action
	C13 Monitoring, logging & anomaly detection	Append-only signed decision log is the substrate
	C14 Human oversight & trust	HOLD outcomes route to human approval; replay reconstruction available
NIST SP 800-207	§2.1 Tenets 1-3	Resource access subject to dynamic policy
	§2.1 Tenet 6	All access authenticated and authorized
	§3.3 Identity	Cryptographic actor identity binding
	§3.4.1 Resource access	Authority is the PDP for autonomous agent actions
NIST AI Agent Security RFI	2026-00206 PAA	Architectural reference for Pre-Action Authorization
IEEE 7001-2021 (published)	Transparency of autonomous systems	Signed decision artifacts with content-hashed policy; reproducible replay
IEEE 7009-2024 (published)	Fail-safe design	Default-deny, fail-closed on authority unavailability
IEEE 7003-2024 (published)	Algorithmic bias considerations	Append-only signed log as substrate for population-level bias analysis
IEEE P7009.1 (draft)	Safety management — anomalous-behavior interventions	HOLD outcomes designed as the formal intervention primitive
IEEE P7022 (draft)	Trustworthy generative & agentic AI in enterprise	Designed against the gaps this draft identifies: agentic AI governance with forensic audit substrate
IEEE P2863 (draft)	Organizational governance of AI	Designed as a technical complement to organizational principles and processes in P2863/D2 (March 2026). Founder has submitted formal line-item comments to the working group; not adopted or endorsed

Standard	Specific reference	How Synchronicity maps
IEEE P3301 (draft, working group)	UIS / MACR / EGA	Founder is a working-group participant; no endorsement or conformity claim
NIST SP 800-53	AU-9 Audit log protection	Append-only signed log, signature verification
	SI-4 System monitoring	Authority as hardened control plane
	CP-2 Contingency planning	Service availability monitor, fail-closed
	SC-36 Distributed processing	Edge-native offline verification
GDPR / ISO/ IEC 27701	GDPR Arts. 44-50, ISO 27701	Jurisdictional attributes in SPADs
SOC 2	CC6.1	Tenant-scoped policy at evaluation time
IEC 62443	Industrial control systems	Air-gapped, offline-capable governance

Scope of claims

Synchronicity provides the **technical control substrate** that conformity claims rest on. The organizational management system around those controls — documented processes, audited evidence, notified-body assessment, stakeholder engagement — remains the responsibility of the deploying organization, in partnership with their auditor.

This separation is deliberate. The same architecture supports an ISO 42001 certification effort, an EU AI Act conformity assessment under Art. 40, and a NIST AI RMF alignment claim for U.S. federal procurement, without overpromising on any of them.

About

Synchronicity is a product of Keystone Digital Holdings LLC. The founder is a contributor to OWASP AISVS (controls C9.7.7, C5.6.5, C5.6.6) and has submitted formal responses to the NIST AI Agent

Security RFI (2026-00206) and NIST COSAiS. Patent applications pending. Patent counsel: Schwegman Lundberg & Woessner.

For an architecture briefing under NDA: boone.carlson@keystonedigitalholdingsgroup.com

---