Acquisition Brief - RealityIntegrity.com

Asset offered

• Domain name: RealityIntegrity.com (.com, exact-match)

• Nature: descriptive digital asset, reserved as a neutral, vendor-independent banner for the emerging cross-sector capability “Reality Integrity”, i.e., preserving and verifying the integrity of “reality signals and representations” across synthetic media, sensors, logs, digital twins, and automated decisions, with evidence suitable for audit, investigations, and governance.

• Not included:

o no audit, consulting, legal, compliance, security, forensic, or certification service,

o no standard-setting authority, no accreditation, no official label,

o no software, datasets, indices, methodology, registry, “trust list”, or operational platform,

o no claim of truth, authenticity, correctness, safety, or regulatory compliance,

o no endorsement of any standard, vendor, product, or public institution.

Contacts (suggested)

• Site: https://www.realityintegrity.com

• Email: contact@realityintegrity.com

• LinkedIn: https://www.linkedin.com/company/realityintegrity (if applicable)

This document - who is it for, why

This brief is intended for a C-suite / Board decision committee:

• CEO, CFO, COO, CRO, CISO, CTO, CIO, Heads of Risk / Assurance / Compliance,

• Trust & Safety leadership, Content Integrity / Media Forensics / Fraud / Investigations teams,

• AI Governance, Digital Risk, Data & Platform teams, Identity / Access / Logging stakeholders,

• General Counsel / Compliance, Corporate Development, M&A, Partnerships,

• Public-interest initiatives, standards and multi-stakeholder coalitions.

Purpose: assess whether RealityIntegrity.com should be secured as a category-grade banner for an institutional initiative centered on integrity of reality-linked signals, provenance and disclosure, and audit-ready evidence for high-stakes digital interactions.

This document is informational only. It is not legal, compliance, audit, security, financial, or investment advice.

Disclaimers (must remain identical across site and documents)

“RealityIntegrity.com is an independent, informational resource. It is not affiliated with any government entity, standards body, certification authority, or commercial provider.”

“Nothing on this site constitutes legal, compliance, audit, or security advice. Consult qualified professionals and primary sources.”

“The domain RealityIntegrity.com may be available for institutional partnership or acquisition by qualified entities.”

1. Decision in one page

What it is

RealityIntegrity.com is a category-grade .com designed to name a structural trust requirement: the ability to preserve and verify the integrity of “reality signals and representations” across synthetic media, sensors, logs, and automated decisions.

“Reality Integrity” applies whenever decisions, liability, compliance, or investigations depend on whether a record reflects an authorized event and a disclosed lifecycle of transformations.

Category definition (short)

Reality Integrity is the property that a reality-linked signal or representation remains trustworthy throughout its lifecycle (capture or creation, transformation, transmission, storage, and use), with verifiable provenance where available and disclosed changes within a defined scope and threat model.

Key attributes (non-technical)

• Integrity is managed as a lifecycle property, not an afterthought.

• Transformations are disclosed and traceable, not hidden.

• Evidence is reviewable by independent internal or external parties.

• Evidence is tamper-evident or tamper-resistant where feasible.

• Evidence supports post-incident reconstruction and dispute handling.

• Claims are explicit about boundaries: what can be proven, what can be evidenced, and what remains an assumption.

Why it matters now

• Synthetic generation and automated manipulation break default trust in media and records.

• Regulation and procurement language increasingly emphasize traceability, marking, and evidence.

• Provenance standards are moving from “specification” to operational governance (conformance, trust infrastructure).

• Cybersecurity and public-interest ecosystems are framing integrity as a prerequisite for investigations, safety, and resilience.

• Platform-scale information flows and agentic workflows require durable decision trails.

What it is not (anti-confusion)

Reality Integrity is not: a product, a certification, a regulator program, a standards body, a “truth authority”, or a vendor claim. It is not a single technology (watermarking,

cryptography, AI detection, blockchain, etc.). It is not censorship or content adjudication.

What can enable it (illustrative)

• Provenance credentials and cryptographic binding (signatures, manifests, metadata integrity)

• Disclosure and labeling mechanisms (human- and machine-readable)

• Trust infrastructures (certificate policies, trust lists where applicable, verification transparency)

• Secure capture and device identity (including sensor provenance where relevant)

• Append-only logs, audit trails, and integrity-preserving storage

• Verification toolchains and repeatable checks

• For high-assurance contexts: hardware roots of trust, attestation, or other integrity anchors

Why the domain is strategic

“Integrity” is an institutional governance word that scales across sectors and withstands legal and procurement scrutiny. “Reality” elevates scope beyond AI media to include sensors, logs, digital twins, and operational representations. The phrase sits above vendors and below policy and liability decisions, making it suitable for coalitions, regulators’ reference ecosystems, and cross-industry governance.

Safety posture (institutional compatibility)

Independent informational resource. No services offered. No claim of certification, authority, or official standard. Clear disclaimers. Acquisition scoped to the domain name only.

---

2. What RealityIntegrity.com is / is not

2.1 Scope (where the category naturally applies)

• Synthetic media used as evidence: claims, disputes, investigations, journalism, public-interest records

• Platform-scale trust and safety: provenance signals, labeling, integrity workflows

• High-liability workflows: regulated reporting, compliance artifacts, audit trails, contract evidence

• Sensor and measurement integrity: industrial monitoring, security contexts, scientific imaging

• Digital twins and operational representations: change tracking, provenance of updates and inputs

• Agentic and automated decision systems: inputs/outputs, logs, and decision traces that must be reviewable

2.2 What it is not

• Not an audit firm, not a certification authority, not a regulator, not a standards body

• Not a promise of truth, authenticity, safety, compliance, or “proof of reality”

• Not an enforcement program, registry, or trust list operator unless a future owner builds one independently

• Not a commercial tool, platform, dataset, or service layer unless developed by the acquirer

---

3. Buyer set (who can rationally own it)

Audit and Assurance

• Global audit networks, trust services, assurance practices expanding into AI/media integrity evidence and governance

Platform trust, safety, and provenance infrastructure

• Platforms and infrastructure providers implementing provenance, credentials, labeling, and verification workflows at scale

Cybersecurity, resilience, and investigations ecosystems

• Security vendors and incident response leaders where integrity evidence underpins investigations and liability handling

Regulated industries and high-liability operators

• Finance, healthcare, critical infrastructure, defense supply chains, and regulated reporting where integrity evidence becomes non-optional

Public-interest institutions and multi-stakeholder initiatives

• Coalitions and observatories that need neutral category language across competing vendors and jurisdictions

Risk governance and insurance ecosystems (without offering insurance)

• Risk frameworks, prerequisites, fraud prevention, and evidence handling where integrity affects exposure and decision-making

Typical sponsors

CISO, CRO, CTO, Head of Trust & Safety, Head of Assurance, Head of AI Governance, General Counsel / Compliance leadership, Corporate Development.

---

4. Deployment options (examples, non-prescriptive)

A. Reference hub (public, neutral)

Definitions, glossary, taxonomy of integrity mechanisms, and curated primary references (regulatory and standards).

B. Standards and governance landscape map

Neutral mapping of provenance, labeling, credential ecosystems, conformance programs, and institutional terminology.

C. Evidence taxonomy and implementation patterns library

Threat-model framing, evidence quality grading, and lifecycle integrity patterns (media, sensors, logs, agents).

D. Coalition or program banner

A neutral banner to convene stakeholders around integrity requirements, interoperability, verification procedures, and procurement language.

---

5. Acquisition process (domain name only)

Typical institutional flow: NDA → strategic discussion → formal offer → escrow → domain transfer.

Unless explicitly agreed otherwise, the transaction covers only the RealityIntegrity.com domain name as an intangible digital asset. No software, datasets, indices, consulting, lobbying, infrastructure, licence, registry, or service layer is included.

Initial contact for serious enquiries: contact@realityintegrity.com

Appendix: primary references (for the Evidence Pack)

• EU: Code of Practice on marking and labelling of AI-generated content (Article 50 alignment)

• C2PA: Conformance Program and Trust List governance materials

• National cybersecurity / inter-agency guidance on Content Credentials and multimedia integrity

• UN: Global Principles for Information Integrity