



Actif proposé

- Nom de domaine : RealityIntegrity.com (.com, exact-match)
- Nature : actif numérique descriptif, réservé comme bannière neutre et indépendante pour la capacité transversale « Reality Integrity », c'est-à-dire préserver et vérifier l'intégrité de ce qui sert de "réalité opérationnelle" (contenus synthétiques, signaux capteurs, logs, jumeaux numériques, décisions automatisées), avec des éléments de preuve exploitables en audit, enquête, litige et gouvernance.
- Ne sont pas inclus :
 - o aucun service d'audit, de conseil, juridique, conformité, cybersécurité, forensics, ou certification,
 - o aucune autorité de standardisation, aucune accréditation, aucun label officiel,
 - o aucun logiciel, base de données, index, méthodologie, registre, "trust list", ni plateforme opérationnelle,
 - o aucun engagement sur la vérité, l'authenticité, l'exactitude, la sécurité ou la conformité,
 - o aucune approbation d'un standard, d'un fournisseur, d'un produit ou d'une institution.

Contacts (suggestion)

- Site : <https://www.realityintegrity.com>
- Email : contact@realityintegrity.com
- LinkedIn : <https://www.linkedin.com/company/realityintegrity> (si applicable)

Ce document - pour qui, pourquoi

Ce brief est destiné à un comité de décision C-suite / Board :

- CEO, CFO, COO, CRO, CISO, CTO, CIO, responsables Risk / Assurance / Compliance,
- directions Trust & Safety, Content Integrity / Media Forensics / Fraude / Investigations,
- équipes Gouvernance IA, Risque digital, Data/Plateforme, Identité/Accès/Logs,
- Juridique/Compliance, Corporate Development, M&A, Partenariats,
- initiatives d'intérêt général, coalitions multi-acteurs et écosystèmes de standards.

Objet : évaluer si RealityIntegrity.com doit être sécurisé comme bannière category-grade pour une initiative institutionnelle centrée sur l'intégrité des signaux et représentations du réel, la provenance et la disclosure, et la preuve "audit-ready" dans des environnements à responsabilité élevée.

Ce document est informatif. Il ne constitue ni un avis juridique, ni un avis de conformité, ni un avis d'audit, ni un avis de sécurité, ni une recommandation financière ou d'investissement.

Disclaimers (à conserver identiques partout)

"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. Décision en une page

Ce que c'est

RealityIntegrity.com est un .com category-grade conçu pour nommer une exigence de confiance devenue structurelle : préserver et vérifier l'intégrité des "signaux et

représentations du réel” (médias, capteurs, logs, jumeaux numériques, décisions automatisées) dans un monde où la génération et la modification à grande échelle deviennent la norme.

« Reality Integrity » s’applique dès lors que des décisions, des obligations, des audits, ou des responsabilités dépendent de la capacité à démontrer ce qui a été capté/produit, ce qui a changé, et dans quelles limites.

Définition courte

Reality Integrity est la propriété qu’un signal ou une représentation liée au réel reste fiable tout au long de son cycle de vie (capture/création, transformations, transmission, stockage, usage), avec une provenance vérifiable quand elle existe et des transformations divulguées, dans un périmètre et un modèle de menace définis.

Attributs clés (sans jargon)

- L’intégrité est pensée comme une propriété “cycle de vie”, pas comme un patch.
- Les transformations sont divulguées et traçables, pas invisibles.
- Les preuves sont examinables par des tiers (internes/externes).
- Les preuves sont résistantes à la falsification ou au minimum détectables si altérées.
- Les preuves permettent reconstitution post-incident et gestion des contestations.
- Les limites sont explicites : prouvable, seulement attestable, ou hypothèse.

Pourquoi maintenant

- Les contenus synthétiques et la manipulation automatisée détruisent la confiance par défaut.
- Les cadres de conformité et les achats institutionnels convergent vers traçabilité, marquage, preuves.
- Les standards de provenance passent de “spécification” à gouvernance opérationnelle (conformance, infrastructures de confiance).
- Les écosystèmes cybersécurité et intérêt général cadrent l’intégrité comme prérequis d’enquête, de sûreté et de résilience.
- Les plateformes et les workflows agentiques exigent des traces durables et auditable.

Ce que ce n'est pas (anti-confusion)

Reality Integrity n'est pas : un produit, une certification, un programme gouvernemental, un organisme de normalisation, une "autorité de vérité", ni une revendication fournisseur. Ce n'est pas une technologie unique (watermarking, crypto, détection IA, blockchain, etc.). Ce n'est pas de la censure ni de l'arbitrage éditorial.

Ce qui peut l'activer (illustratif)

- Provenance et credentials (métadonnées signées, manifests, intégrité cryptographique)
- Disclosure et labelling (signaux lisibles humains et machines)
- Infrastructures de confiance (politiques de certificats, trust lists selon cas, vérification)
- Capture sécurisée et identité des dispositifs (dont provenance au niveau capteur si pertinent)
- Journaux append-only, audit trails, stockage préservant l'intégrité
- Toolchains de vérification et contrôles reproductibles
- En haute assurance : racines matérielles de confiance, attestation, ancrages d'intégrité

Pourquoi le domaine est stratégique

« Integrity » est un mot de gouvernance durable, compatible compliance, audit, risque, et achats institutionnels. « Reality » élargit au-delà de l'IA vers capteurs, logs, jumeaux numériques et représentations opérationnelles. L'expression se situe au-dessus des solutions et au-dessous des décisions de risque, ce qui en fait une bannière acceptable par des coalitions et des initiatives multi-acteurs.

Posture de sécurité (compatibilité institutionnelle)

Ressource informative indépendante. Aucun service proposé. Aucune revendication d'autorité, de certification ou de standard officiel. Disclaimers explicites. Acquisition focalisée sur le nom de domaine uniquement.

2. Ce qu'est / n'est pas RealityIntegrity.com

2.1 Périmètre naturel (exemples)

- Médias synthétiques utilisés comme preuve : sinistres, litiges, enquêtes, information d'intérêt public
- Trust & Safety à l'échelle plateforme : provenance, signaux, labelling, workflows de vérification
- Environnements régulés et à responsabilité : reporting, preuves contractuelles, audit trails
- Intégrité capteurs et mesures : industrie, sécurité, imagerie scientifique
- Jumeaux numériques et représentations opérationnelles : suivi des changements et provenance des mises à jour
- Systèmes agentiques : entrées/sorties, logs, traces de décision examinables

2.2 Ce que ce n'est pas

- Ni cabinet d'audit, ni autorité de certification, ni régulateur, ni organisme de normalisation
 - Ni promesse de vérité, d'authenticité, de sûreté, de conformité, ou de "preuve totale"
 - Ni programme d'exécution, registre, trust list, ou service tiers sauf développement autonome par l'acquéreur
 - Ni outil commercial, plateforme, dataset ou service sauf développement autonome par l'acquéreur
-

3. Acheteurs naturels (logique d'acquisition)

Audit & Assurance

- Réseaux d'audit et practices trust/assurance étendant leurs offres vers preuves d'intégrité (IA, médias, gouvernance)

Plateformes, Trust & Safety et infrastructures de provenance

- Acteurs déployant provenance, credentials, labelling et vérification à grande échelle

Cybersécurité, résilience et investigations

- Acteurs où la preuve d'intégrité conditionne les enquêtes, la gestion de crise et la responsabilité

Industries régulées et environnements à forte responsabilité

- Finance, santé, infrastructures critiques, supply chain défense, secteurs où l'intégrité devient non-optionnelle

Institutions d'intérêt général et coalitions multi-acteurs

- Observatoires, initiatives public-privé, consortiums nécessitant une bannière neutre au-dessus des fournisseurs

Gouvernance du risque et écosystèmes assurance (sans vendre d'assurance)

- Cadrage risque, prérequis de preuve, antifraude et gestion d'exposition où l'intégrité influence les décisions

Sponsors typiques

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

4. Déploiements possibles (exemples, non prescriptifs)

A. Hub de référence (public, neutre)

Définitions, glossaire, taxonomie des mécanismes d'intégrité, et références primaires (régulation + standards).

B. Cartographie standards et gouvernance

Cartographie neutre des écosystèmes provenance/credentials/labelling, conformance et infrastructures de confiance.

C. Bibliothèque de patterns et taxonomie de preuve

Cadrage threat model, qualité de preuve, patterns cycle de vie (médias, capteurs, logs, agents).

D. Bannière de coalition ou de programme

Bannière neutre pour fédérer sur exigences d'intégrité, interopérabilité, procédures de vérification et langage d'achat.

5. Process d'acquisition (nom de domaine uniquement)

Process type : NDA → échanges stratégiques → offre formelle → escrow → transfert du domaine.

Sauf accord explicite contraire, la transaction porte uniquement sur le nom de domaine RealityIntegrity.com en tant qu'actif numérique incorporel. Aucun logiciel, base de données, index, conseil, lobbying, infrastructure, licence, registre, ou service n'est inclus.

Contact initial pour échanges sérieux : contact@realityintegrity.com

Annexe : références primaires (pour l'Evidence Pack)

- UE : Code of Practice "marking and labelling" (alignement Article 50)

- C2PA : Conformance Program + gouvernance Trust List
- Guidance cybersécurité / inter-agences sur Content Credentials et multimedia integrity
- ONU : Global Principles for Information Integrity