Acquisition Brief (EN) - ComputeIntegrity.com (2025-11)

1) Asset snapshot

Asset: ComputeIntegrity.com
Type: Descriptive .com domain name
Status: Available for acquisition (domain as an intangible digital asset)
Intended positioning: Neutral, non-vendor, category-grade banner for the concept of compute integrity
Contact: contact@computeintegrity.com (for NDA and acquisition discussions)

Important notice (scope and safety):
ComputeIntegrity.com is a descriptive digital asset. It is not an official portal and has no affiliation with any regulator, standards body, public authority, or private company. It provides no cybersecurity service, no audit, no certification, no compliance assessment, no penetration testing, and no legal, regulatory, or security advice. Any future use would be entirely designed, governed, and operated by the acquirer under its own responsibilities and applicable laws. All trademarks belong to their respective owners.

---

2) The category

Compute integrity can be described as the ability to demonstrate that a computing environment is running the intended software on a trustworthy platform, without unauthorized modification, and that this state can be attested in a way that relying parties can verify.

In practical terms, compute integrity sits beneath critical digital trust outcomes:

- cloud and edge workloads that must prove they are unmodified
- regulated or high-assurance systems that require evidence for procurement and assurance
- AI and automated decision systems where provenance and trust increasingly depend on verifiable execution conditions

Compute integrity is not a product category owned by one vendor. It is an infrastructure requirement that can become contractual language across markets.

---

3) Where it exists today (descriptive reality)

Compute integrity is already present in real systems through widely used technical patterns and assurance concepts, including:

- measured boot and chain-of-trust approaches that record integrity measurements
- hardware-rooted trust mechanisms (for example TPM-based measurement and related approaches), used as building blocks rather than a single solution
- remote attestation concepts where an external verifier can validate claims about the state of a device or workload
- integrity verification as a governance and assurance expectation in critical deployments

This brief intentionally avoids operational guidance. The point is the category: the language that describes why integrity evidence matters and how it is verified at a high level.

---

4) Why now

Compute integrity is moving from engineering concern to executive and procurement language due to three converging forces:

A) Digital sovereignty and resilience expectations
Governments, critical industries, and large enterprises increasingly treat integrity as a resilience prerequisite. The question shifts from “is the system secure” to “can the system prove, continuously and verifiably, that it is not compromised.”

B) Supply chain and compliance pressure in Europe
European cyber and product-security obligations are trending toward stronger assurance expectations over time, especially for digital products and connected systems. Regardless of precise timelines, the market trajectory is clear: procurement, liability, and conformity narratives push toward measurable and attestable integrity properties.

C) AI deployment at scale
As AI systems become embedded in operations, the trust problem expands. Even if an output is signed or logged, stakeholders still ask: was the environment that produced it

trustworthy. Compute integrity becomes the foundation layer that supports higher-level guarantees like signed outputs, verifiable logs, and auditability.

---

5) What this name can become (without promising a product)

ComputeIntegrity.com can anchor a neutral category banner that supports several credible, non-commercial forms of stewardship:

- a taxonomy and vocabulary hub for compute integrity and attestation concepts
- a reference index mapping how compute integrity is described across standards, guidance, and procurement language
- an observatory that curates public resources, definitions, and non-controversial frameworks
- a governance framing layer linking integrity evidence to assurance, risk, and procurement requirements

The asset is the domain name. Any framework, portal, index, or stewardship model would be created and governed by the acquirer.

---

6) Buyer archetypes (non-exhaustive)

ComputeIntegrity.com is relevant to buyers who benefit from a neutral banner and category ownership, including:

Infrastructure and cloud ecosystem

- hyperscalers and cloud platforms
- confidential computing and trusted execution ecosystem participants
- edge computing and industrial compute platforms

Cyber assurance and compliance ecosystem

- assurance and audit-adjacent groups (non-regulated positioning only)
- security governance organisations and industry coalitions
- integrators supporting critical infrastructures

Public sector and strategic programmes

- multi-stakeholder initiatives around digital resilience and critical infrastructure
- research institutes, foundations, or standards-adjacent organisations that may host neutral knowledge hubs

Technology governance and risk

- organisations building frameworks connecting integrity evidence to governance, risk, and procurement language

This is not a claim that these actors will buy. It defines who could legitimately steward such a category banner.

---

7) Why this exact name

Clarity: “Compute Integrity” is direct, board-readable language that still maps to technical reality.
Breadth: It does not narrow the concept to a single protocol or vendor approach.
Category lock: It is a natural label for a space that can become a standard phrase in procurement and assurance narratives.
Durability: It remains relevant across cloud, edge, embedded systems, and AI deployment cycles.
Neutrality: It can credibly host a non-vendor observatory without implying a commercial offering.

---

8) Risk controls (litigation and reputation minimisation)

ComputeIntegrity.com can be positioned with low dispute risk when the following guardrails are applied consistently:

Non-affiliation: No suggestion of official status, endorsement, partnership, or certification.
No services: No offer of pentesting, audit, compliance, certification, or security operations.
No sensitive claims: No “guarantees,” no “compliance assured,” no “certified by.”
Descriptive-only design: Neutral aesthetics, no institutional mimicry, no logos of third parties.
Clear disclaimers: Visible on every page, plus a longer disclaimer page if needed.
Trademark respect: Explicit statement that all trademarks belong to their respective owners.

---

9) Acquisition pathway (secure and professional)

A typical institutional process:

1. discreet enquiry and qualification of interest

2. NDA where appropriate
3. strategic discussion on intended stewardship and perimeter
4. formal written offer
5. escrow process to secure payment and transfer
6. registrar transfer and DNS handover to the acquirer

Unless explicitly agreed otherwise, the transaction covers only the ComputeIntegrity.com domain name as an intangible asset.

---

10) Valuation framing (scenarios, not promises)

Valuation depends on whether "compute integrity" becomes mainstream procurement and governance language across Europe and global markets, and whether the buyer values category ownership and defensive positioning.

Illustrative scenarios only:

- **Base case:** category used in technical circles and selective procurement language
- **Upside case:** category becomes widely used governance term across cloud, critical systems, and AI assurance
- **Strategic case:** domain becomes a central banner for a neutral observatory or widely referenced framework

No sale outcome is promised. The asset is positioned to be defensible, neutral, and category-grade if adoption accelerates.