AIVO Standard

Global Governance Standard for AI Visibility Data Integrity

AIVO Data Integrity & Verification Methodology (DIVM)

Version 1.0 — October 2025

Establishing reproducible, auditable, and legally sound data standards for enterprise AI visibility reporting.

Published by: AIVO Standards Division

Official Release Date: 22 October 2025
DIVM v1.0 — Document SHA-256

Hash: c6f8766b2ffd7a76851af4787b6110c5b1e8436ac72fbaf77e470001c2f8a602

For verification, visit: https://aivostandard.org

Table of Contents

3. Data Integrity Framework

3.1 Definition of Data Integrity in AI Visibility
3.2 Live LLM Interrogation Standards
3.3 Data Provenance and Metadata Requirements
3.4 Source Tiering (Tier 1–3)
3.5 Provenance Chain and Chain of Custody
3.6 Acceptable vs. Non-Acceptable Data Sources

4. Measurement & Reproducibility Standards

4.1 Sampling Framework and Statistical Reliability
4.2 Confidence Intervals (CI)
4.3 Coefficient of Variation (CV)
4.4 Intra-Class Correlation (ICC)
4.5 Replay Harness and Reproducibility Testing
4.6 Statistical Tolerance (±5%)
4.7 Temporal Consistency and Model Versioning

5. Data Governance, Security & Compliance

5.1 Governance Roles and Responsibilities
5.2 Information Security Alignment (ISO 27001, 27701)
5.3 Privacy and DPIA Considerations
5.4 Audit Trail and Evidence Preservation
5.5 Incident Response and Escalation
5.6 Data Retention and Archival Policy

6. Transparency, Verification & Assurance

6.1 Disclosure Requirements
6.2 Transparency Levels (1–3)
6.3 Standard Disclosure Pack
6.4 Third-Party Assurance and Replay Verification
6.5 Integration with ESG and Regulatory Reporting
6.6 Trust Seals and Assurance Levels

7. Implementation & Operationalization

7.1 Integration with AIVO Metrics (PSOS, QSCR, Decay)
7.2 Implementation Lifecycle Framework
7.3 DIVM Compliance Checklist
7.4 Versioning & Change Management
7.5 Integration with Enterprise Governance
7.6 Operational Roles & Responsibilities
7.7 Automation Pathways
7.8 Escalation & Exception Handling
7.9 Recommended Implementation Timeline
7.10 Summary of Implementation Requirements

8. Appendix

8.1 Glossary of Core Terms
8.2 Example Metadata Schema (with model version reference)
8.3 Regulatory Timeline (2025–2027)
8.4 Verification Report Template
8.5 Regulatory & Standards Crosswalk
8.6 Example Fragility & Drift Calculation
8.7 Example Replay Log Extract
8.8 Sample Transparency Disclosure Table
8.9 Recommended Escalation Thresholds
8.10 Contact & Certification Framework
8.11 Formal Reference List
8.12 Standards Mapping Annex

Document Control & Versioning

Field	Value
Document Title	AIVO Data Integrity & Verification Methodology (DIVM)
Version	1.0
Release Date	2025-10-22
Status	Final
Classification	Public / Enterprise / Regulatory
Prepared By	AIVO Standards & Methodology Group
Approved By	AIVO Governance Council
Next Scheduled Review	2026-04
Document Owner	AIVO Standards Division
Distribution	Partner network, assurance providers, regulators, enterprise clients

Change History

Version	Date	Description	Author	Approved By
0.1	2025-09-15	Initial working draft	Standards Group	—
0.5	2025-10-05	Expanded regulatory sections	Standards Group	Governance Council
0.9	2025-10-20	Added replay harness & assurance	Standards Group	Governance Council
1.0	2025-10-22	Final published version	Standards Group	Governance Council

Versioning Policy

- All major changes to DIVM must result in a **new version number** (e.g., 2.0, 3.0).
- Minor editorial or clarifying changes will be logged as **incremental versions** (e.g., 1.1, 1.2).
- All methodology versions must be **archived with date, version, and hash**.
- Any third-party assurance report must reference the **exact DIVM version** used at the time of measurement.
- When LLM model upgrades materially affect methodology (e.g., new inference behaviors, retrain cycles), a **version increment** must be issued.
- Major regulatory updates (e.g., changes to the AI Act or ISO standards) will also trigger new major or minor versions as appropriate.

Document Hashing

To prevent tampering and ensure authenticity:

- Each published DIVM version will carry a **SHA-256 document hash**.
- Hashes will be logged in AIVO's public standards registry.
- External auditors and partners can verify the integrity of any document version.

Document SHA-256 Hash

c6f8766b2ffd7a76851af4787b6110c5b1e8436ac72fbaf77e470001c2f8a602

Foreword

Artificial intelligence is rapidly reshaping how brands are discovered, recommended, and trusted. As large language models (LLMs) become the primary interface between users and information, **brand visibility is no longer determined by search rankings alone** — it is determined by what AI assistants say, recommend, and surface.

This shift creates a fundamental new requirement: **verifiable, reproducible visibility data** that can be trusted by enterprises, investors, regulators, and auditors.

Most current visibility dashboards rely on opaque methods — often based on scraped SERPs, cached outputs, or non-reproducible telemetry. These approaches may offer superficial insight but cannot support corporate governance, regulatory compliance, or investor reporting.

The **AIVO Data Integrity & Verification Methodology (DIVM)** is designed to change this. DIVM establishes a **governance-grade data integrity framework** that ensures every visibility metric produced under AIVO Standard can be **proven, reproduced, and defended**.

DIVM is not a tool — it is the **standard against which tools should be measured**. It provides the technical, statistical, and legal scaffolding required to turn visibility reporting into an auditable asset.

About AIVO Standard

AIVO Standard defines how brand presence is detected, measured, and governed within major AI ecosystems.
It combines **live LLM interrogation**, **trust-weighted prompt-space scoring**, and **fragility and decay modelling** to give enterprises a precise and predictive view of their AI visibility position.

Unlike traditional dashboards, AIVO does not infer visibility from search engine signals — it **measures it directly inside AI assistants**, where buyer intent is increasingly captured.

DIVM underpins this measurement system by providing:

- A verifiable data integrity foundation,
- A consistent methodology aligned with international standards,
- A clear governance framework to satisfy compliance, regulatory, and board-level assurance needs.

This combination transforms visibility data from a marketing indicator into a **board-grade metric**.

Purpose of DIVM

The purpose of DIVM is to **establish a standardized, globally applicable framework for the collection, verification, and reporting of AI visibility data**.

This framework ensures that:

- All measurements are derived from **live, attributable model interactions**,
- All data points are supported by **transparent provenance and chain of custody**,
- Reported results meet strict **reproducibility and statistical integrity criteria**,
- Outputs can withstand scrutiny from regulators, auditors, investors, and legal bodies.

DIVM is designed to **future-proof enterprise AI visibility reporting** against tightening regulatory environments such as EU Artificial Intelligence Act, Colorado Artificial Intelligence Act, EU Cyber Resilience Act, and EU Data Act.

Scope

DIVM applies to **all visibility measurements derived from live LLM interrogations** across major AI platforms, including but not limited to:

- Generative search and assistant products,
- Prompt-space analysis and slot occupancy measurement,
- Citation and trust signal mapping,
- Fragility, decay, and drift modelling.

The methodology governs:

- How data is collected,
- How provenance is recorded and protected,
- How metrics are statistically validated,
- How disclosures are structured for audit, regulatory, and assurance use cases.

It applies globally and is adaptable to different industry verticals, regulatory contexts, and enterprise risk frameworks.

Intended Audience

DIVM is designed for organizations and stakeholders that require **trustworthy, defensible AI visibility intelligence**, including:

- **Enterprises & PLCs** — for board-level reporting, competitive strategy, and regulatory readiness.
- **Auditors & Assurance Providers** — to independently verify and attest to data accuracy and reproducibility.
- **Regulators & Compliance Bodies** — to assess the trustworthiness of AI visibility reporting against legal and ethical frameworks.
- **Procurement & ESG Teams** — to evaluate vendor claims, verify governance posture, and meet disclosure obligations.
- **Investors & Financial Analysts** — to assess visibility exposure and opportunity in capital markets and valuations.

1. Introduction & Principles

1.1 Why Data Integrity Matters in AI Visibility

The global information landscape is undergoing a structural shift.
Traditional search engines are no longer the primary discovery layer for products, services, and brands. Instead, **AI assistants are becoming the default discovery interface** — answering questions, making recommendations, and shaping perception through conversational interfaces.

For enterprises, this means **visibility is no longer what appears in search results** — it's what **AI systems say**.
That shift introduces profound new risks:

- **Ephemeral visibility:** Positions in AI outputs can shift or disappear entirely overnight as models update, prompting logic evolves, or competing entities strengthen their signals.
- **Opaque methodologies:** Most commercial dashboards rely on scraped search data, cached outputs, or indirect signals, offering no transparency, reproducibility, or assurance.
- **Regulatory exposure:** As AI governance frameworks tighten, unverifiable visibility data can no longer be used to support ESG disclosures, risk filings, or investor reporting.

In this new environment, **data integrity isn't a "nice to have" — it's a legal, strategic, and financial necessity.**

1.2 What DIVM Sets Out to Solve

AIVO Standard is built on **live interrogation of large language models**, **trust-weighted visibility scoring**, and **fragility and decay modelling**.

DIVM provides the **methodological backbone** to make that data:

- **Verifiable** — every data point can be traced to its origin (prompt, model, timestamp, grounding, source tier).
- **Reproducible** — results can be re-run by independent parties and produce materially identical outputs within a defined statistical tolerance.
- **Governance-grade** — outputs can stand up to internal audit, regulatory review, or investor due diligence.

- **Regulation-ready** — aligned with evolving frameworks like EU Artificial Intelligence Act, Colorado Artificial Intelligence Act, EU Cyber Resilience Act, and EU Data Act.

Where typical dashboards deliver **marketing-level visibility scores**, DIVM delivers **defensible evidence**.

1.3 Core Principles of DIVM

DIVM is founded on six guiding principles. These principles shape every requirement, metric, and assurance process in this methodology.

1.3.1 Live Interrogation Over Proxy

All visibility data must originate from **live LLM interrogation** at the time of measurement.

- No scraped search results.
- No cached datasets.
- No third-party proxy APIs.

Every data point must have verifiable metadata (prompt, model, timestamp, locale, and grounding).

1.3.2 Provenance & Transparency

Each data point must carry a **complete, tamper-evident chain of custody**, enabling third parties to verify where, when, and how it was obtained.
Transparency is a governance obligation, not a feature.

1.3.3 Statistical Reproducibility

Results must be independently reproducible within a strict tolerance (e.g., ±5 % confidence interval, ICC ≥ 0.80).
This transforms visibility reporting from subjective interpretation to **objective measurement**.

1.3.4 Trust Over Volume

Traditional SEO rewarded link volume. Early GEO dashboards reward mention volume. DIVM prioritizes **trust signals** (Tier 1 structured, authoritative sources) over volume-based noise, aligning with how AI models increasingly weight grounding and reliability.

1.3.5 Regulatory Alignment by Design

The methodology is designed to be **natively compatible** with global regulatory frameworks.
It embeds privacy (e.g., General Data Protection Regulation), AI governance (EU AI Act, Colorado AI Act), security (EU CRA), and portability (EU Data Act) obligations into the measurement process itself.

1.3.6 Auditability & Assurance

DIVM ensures that outputs can be:

- independently rerun,
- externally audited, and
- formally attested by qualified third parties (e.g., assurance firms or accredited labs).

This is critical for PLCs and enterprises facing board-level reporting and disclosure requirements.

1.4 Positioning DIVM Within the AIVO Standard

DIVM underpins the entire AIVO Standard ecosystem. It ensures that metrics such as:

- Prompt-Space Occupancy Score (PSOS)
- Quantum Slot Collapse Risk (QSCR)
- Decay and fragility modelling
- Tier-weighted citation analysis

…are not just powerful — they're **verifiable, reproducible, and legally defensible**.

This positions AIVO as the **governance benchmark**, not just another dashboard.
It enables enterprises to confidently integrate AI visibility reporting into:

- Regulatory disclosures,
- Investor relations,
- M&A due diligence,
- Risk registers, and
- Board-level strategic planning.

2. Legal, Regulatory & Standards Alignment

DIVM is designed to function as a **globally credible framework** for AI visibility measurement and assurance.
This requires alignment not only with technical best practices but also with the **legal, regulatory, and data governance regimes** that govern enterprise AI adoption worldwide.

Rather than retrofitting compliance later, DIVM is **natively designed** to meet and exceed the expectations of privacy law, AI governance frameworks, cybersecurity regulation, and international standards.

2.1 Global Privacy & Data Protection Frameworks

DIVM respects and aligns with leading international privacy and data protection frameworks.
Although AIVO does not typically process personal data, **enterprises and PLCs deploying AIVO-based outputs must comply with these frameworks**, especially in cross-border contexts.

Key frameworks:

- **General Data Protection Regulation (GDPR)** — EU regulation governing personal data processing, transparency, and lawful basis.
    - Relevant to provenance, data minimization, retention, and cross-border flows.
- **California Consumer Privacy Act (CCPA)** and **California Privacy Rights Act (CPRA)** — U.S. state laws with GDPR-like opt-out and disclosure obligations.
- **Lei Geral de Proteção de Dados (LGPD)** — Brazil.
- **Personal Information Protection and Electronic Documents Act (PIPEDA)** — Canada.
- **Act on the Protection of Personal Information (APPI)** — Japan.
- **Privacy Act 1988** — Australia (under reform).
- **Personal Data Protection Act (PDPA)** — Singapore.
- **EU-U.S. Data Privacy Framework and Standard Contractual Clauses (SCCs)** — for compliant cross-border data transfers.

DIVM alignment includes:

- Explicit **data minimization and non-PII design** wherever possible.
- Transparent provenance logging that satisfies “right to explanation” requirements.
- Optional Data Protection Impact Assessment (DPIA) templates for enterprises deploying AIVO within regulated environments.

2.2 AI Governance & Risk Frameworks

DIVM is designed with upcoming AI governance regulations in mind — ensuring that **data used in visibility reporting can withstand legal, regulatory, and assurance scrutiny**.

EU AI Act (implementation 2026)

- Defines governance obligations for “high-risk” AI systems, including documentation, risk management, transparency, and human oversight.
- DIVM provides:
    - Complete provenance logs to support AI Act Article 12 (record-keeping).
    - Impact assessment templates aligned with Article 9 (risk management system).
    - Human oversight structure suitable for compliance evidence.

Colorado AI Act (2026)

- Requires deployers of high-risk AI systems to perform **impact assessments** to mitigate algorithmic bias and discrimination.
- DIVM provides:
    - Structured logging of model sources, prompt clusters, and visibility outputs.
    - Standard impact reporting templates enterprises can adapt for state-level compliance.

NIST AI RMF 1.0 (U.S.)

- Voluntary risk management framework focusing on governance, mapping, measurement, and management.
- DIVM aligns through:
    - Transparent provenance (“Map”).
    - Statistical reproducibility and CI reporting (“Measure”).

- Governance hooks and documentation (“Govern”).
- Drift/fragility monitoring and escalation (“Manage”).

OECD AI Principles

- Widely adopted global AI governance baseline — emphasizing transparency, accountability, and robustness.
- DIVM implements these principles operationally through structured evidence and verification.

2.3 Cybersecurity & Data Governance Regulations

EU Cyber Resilience Act (CRA) (2026)

- Requires manufacturers of digital products to:
  - Implement security-by-design measures,
  - Report vulnerabilities within 24 hours,
  - Maintain evidence of security controls.

DIVM readiness includes:

- Hooks for automated vulnerability reporting if AIVO components are classified as “digital elements.”
- Cryptographic integrity measures for provenance logs.
- Clear security governance documentation.

EU Data Act (2026)

- Establishes rules for:
  - Data portability,
  - Interoperability,
  - Switching between providers,
  - Access and sharing obligations.

DIVM readiness includes:

- Standardized **data export formats** (CSV/JSON).
- Full prompt-provenance structure to enable switching and external verification.
- Alignment with enterprise data governance and legal portability requirements.

2.4 ISO and Related Standards

DIVM is explicitly mapped to core international standards to provide **interoperability and external audit readiness**.

Standard	Title	Relevance
ISO 8000	Data Quality	Accuracy, completeness, consistency, provenance
ISO/IEC 5259	Data Quality for Analytics & ML	Structured metadata, reproducibility
ISO/IEC 27001	Information Security Management	Security posture for stored data
ISO/IEC 27701	Privacy Information Management	Data protection governance
ISO/IEC 42001	AI Management Systems	AI governance integration
ISO/IEC Guide 98-3 (GUM)	Uncertainty of Measurement	Confidence intervals and reproducibility
ISO 3534	Statistics Vocabulary	Statistical clarity and interoperability

DIVM adopts a **“referenced standard” model** — aligning with these frameworks without duplicating their language, ensuring that DIVM can be audited or certified by independent assessors against recognized international baselines.

2.5 Provenance & Transparency Frameworks

To support AI governance and reproducibility:

- **W3C PROV**: Standard for expressing provenance information in interoperable formats.
- **Datasheets for Datasets**: Describes dataset composition, collection, and usage context.
- **Model Cards**: Standardized model documentation templates for transparency.

DIVM uses these frameworks to structure:

- Prompt provenance metadata,
- Source and trust tier documentation,
- Transparency annexes for audit and third-party assurance.

2.6 Regulatory Timeline Considerations

Regulation	Effective Year	Key DIVM Alignment
EU AI Act	2026	Full provenance logging, impact assessment, human oversight
Colorado AI Act	2026	Bias and risk assessment template
EU CRA	2026	Vulnerability reporting hook
EU Data Act	2026	Data portability and export
GDPR / Global Privacy Laws	Active	Data minimization, lawful basis, audit logs
NIST AI RMF	Active	Governance and risk management alignment

2.7 Practical Implications for Enterprises

By aligning DIVM with these frameworks, enterprises and PLCs benefit from:

- **Regulatory head start** — ready for AI Act and other obligations years ahead of enforcement.
- **Assurance readiness** — evidence packs designed for audit and compliance submissions.
- **Interoperability** — ability to integrate AIVO reporting into existing ISO, SOC 2, or ESG frameworks.
- **Board confidence** — visibility data that is legally defensible and auditable.

3. Data Integrity Framework

The reliability of any AI visibility measurement depends entirely on the **integrity of its underlying data**.
Unlike traditional dashboards that rely on indirect indicators (e.g., scraped SERPs, proxy APIs, and cached data), DIVM mandates a **direct, structured, and tamper-evident data pipeline** based on live LLM interrogation.

This framework ensures that every number, score, and visibility signal derived through AIVO Standard can be **traced, reproduced, and defended**.

3.1 Data Collection Principles

All data collected for visibility measurements under DIVM must meet **four non-negotiable standards**:

1. **Live Model Interrogation**
    - All visibility measurements must originate from direct API interactions with LLMs.
    - No use of scraped SERPs, cached datasets, or indirect search telemetry.
2. **Deterministic Prompting & Logging**
    - Every prompt issued must be deterministic (i.e., structured, stable wording) and logged in full.
    - Randomization or unlogged prompt variation is prohibited.
3. **Full Metadata Recording**
    - Every response captured must be accompanied by structured metadata (see 3.2).
    - Metadata must be stored in a secure, tamper-evident format.
4. **Regulatory & Ethical Compliance**
    - All collection must align with privacy, AI governance, and security frameworks defined in Section 2.

3.2 Provenance & Chain of Custody

DIVM requires a **verifiable chain of custody** for each measurement.
Each data record must contain the following metadata fields:

Field	Description	Example
prompt_id	Unique identifier for prompt	8a9f1234-…
prompt_text	Exact text of prompt issued	“What are the best hotel chains in Europe?”
model_name	Full name/version of model used	gpt-5.0
model_provider	Source provider	OpenAI
model_version	Model snapshot/version	2025-10-01
temperature	Model temperature setting	0.2
timestamp_utc	ISO 8601 timestamp of call	2025-10-22T15:30:45Z
locale	Locale or region setting	en-GB
response_text	Full model response text	(verbatim output)
citations	URLs/domains cited (if any)	[“wikipedia.org”, “expedia.com”]
source_tiers	Tier classification of cited domains	Tier 1, Tier 2
response_hash	SHA-256 hash of response payload	d7e3...
signature	Optional cryptographic signature for external verification	

This metadata must be:

- **Cryptographically hashed** at capture time.
- **Immutable** — no retroactive edits without creating a new record and linkage.
- **Time-stamped** to the second (UTC).
- **Stored with redundancy** in compliance with applicable retention policies.

This structure allows independent auditors to rerun the exact same prompt, on the same model version, and verify whether the result aligns with reported metrics.

3.3 Source Tiering & Trust Weighting

Not all citations and outputs are equal. DIVM uses **tiering and weighting** to distinguish between trustworthy and weak visibility signals.

Tier Definitions

Tier	Description	Examples	Weight (w)
Tier 1	Structured, authoritative, machine-readable sources	Wikidata, Crunchbase, official .gov or .edu sites, verified brand profiles	1.00
Tier 2	Semi-structured, high-trust third parties	Major media, review platforms with verified identities	0.75
Tier 3	Unstructured / UGC / noise	Reddit, Quora, low-trust domains	0.25

Weighted Visibility Calculation

For each prompt:

$$\text{WeightedVisibilityScore} = \Sigma (\text{MentionCount}_i * w_i) / \text{TotalMentions}$$

Where:

- MentionCount_i = number of mentions from source i
- w_i = weight for tier i

This ensures that a single Tier 1 citation can outweigh multiple Tier 3 mentions, reflecting **real trust weighting inside AI models**, not just raw volume.

3.4 Data Freshness & Cadence

Stale data creates false confidence. DIVM therefore enforces **freshness windows** and cadence standards.

Metric	Definition	Threshold
Maximum Age of Visibility Data	Time since last interrogation of the prompt	≤ 30 days
Minimum Refresh Cadence	Required re-query frequency for active prompts	≥ every 30 days
Drift Check Cadence	Frequency of drift monitoring	Weekly
Decay Warning Trigger	Visibility drop threshold triggering early warning	≥ 15% relative decline over 30 days

Decay Rate Formula

DecayRate = (Visibility_t0 - Visibility_tn) / Visibility_t0
Where:

- Visibility_t0 = initial visibility score
- Visibility_tn = visibility score after n days

If DecayRate ≥ 0.15 (15%), the system flags the prompt as **fragile** and at risk of collapse.

3.5 Drift & Fragility Monitoring

AI visibility is volatile. DIVM includes proactive drift and fragility monitoring as part of its data integrity standard.

Key concepts:

- **Drift**: Gradual change in prompt results over time (e.g., different companies recommended).
- **Collapse**: Sudden disappearance or major rank change.
- **Fragility Index**: A numerical signal indicating how vulnerable a slot is to being replaced.

Drift Detection Method

DriftRate = (Σ |Rank_t0 - Rank_tn|) / N
Where:

- Rank_t0 = initial rank of entity
- Rank_tn = rank after n days
- N = number of prompts monitored
- If DriftRate > 0.20 (20%), the slot is flagged for investigation.
- If DriftRate > 0.35 (35%), automated decay mitigation should be initiated.

3.6 Anti-Tampering and Security Controls

To ensure data integrity at every stage:

- All raw response payloads are **hashed using SHA-256** at the point of capture.
- Audit trails are **immutable** and cryptographically linked.
- Versioning records are stored for each model used.
- Access to raw data is governed by ISO 27001-aligned access controls.
- Optional digital signatures support external verification.

This ensures that **no visibility score can be altered without leaving a forensic footprint**.

3.7 Retention & Archiving

Element	Minimum Retention	Archival Standard
Prompt & response metadata	24 months	Secure encrypted archive
Hash and signature records	24 months	Immutable ledger
Audit logs	36 months	Compliant with GDPR & Data Act

Retention aligns with enterprise audit cycles, procurement requirements, and AI governance documentation under the EU Artificial Intelligence Act.

3.8 Summary of Data Integrity Requirements

Control Area	Requirement	Compliance Indicator
Source Collection	Live interrogation only	100% API call provenance
Metadata Logging	Full structured capture	Mandatory fields populated
Trust Weighting	Tiered + weighted scoring	WeightedVisibilityScore calculation
Freshness & Cadence	Regular refresh and drift monitoring	< 30 days age
Integrity Protection	Hashing, signatures, immutability	SHA-256 verified
Retention	Regulatory-aligned archive	24–36 month lifecycle

4. Measurement & Reproducibility Standards

The credibility of any AI visibility score depends on how reliably it can be **measured, reproduced, and independently verified**.
DIVM establishes strict measurement standards to ensure that all results:

- Are **derived from statistically valid sampling**,
- Include clear confidence and uncertainty metrics,
- Can be **reproduced within an agreed tolerance** by third parties, and
- Are suitable for **board-level and regulatory reporting**.

4.1 Prompt Cluster Sampling Strategy

AI visibility is not defined by a single prompt — it's defined by **prompt clusters** representing user intent across a topic or commercial category.
DIVM mandates a **cluster-based sampling methodology** to achieve statistical robustness and avoid single-prompt bias.

4.1.1 Prompt Categories

Each visibility study must use prompts drawn from one or more of the following **AIVO Prompt Taxonomy** categories:

Category	Description	Example
Intent	Transactional or high commercial intent	"Best hotel chains in Europe"
Conversational	Natural user queries	"Which hotel brands do people trust the most?"
Transactional	Direct buy/convert language	"Book luxury hotel chain in Paris"
Opinion/ Knowledge	General discovery & reputation	"Top recommended hotel chains"

4.1.2 Minimum Cluster Size

Analysis Scope	Minimum Prompts per Cluster	Recommended
Narrow (single niche)	25	50
Standard enterprise	50	100
Multi-region / PLC	100	250

This ensures adequate **Effective Sample Size (ESS)** to support a reproducible visibility score.

4.1.3 Geographic & Linguistic Distribution

- Prompts must reflect the **operational footprint** of the brand (e.g., EN/FR/DE for EU companies).
- Each region must be represented by at least **15% of total prompt volume** in multi-region analyses.
- Localization is not optional — it materially affects LLM output.

4.2 Live Interrogation Requirements

To ensure measurements reflect **current AI assistant output**:

- All prompts must be run through **live LLM calls** at the time of measurement.
- Prompt runs must be **timestamped**, model version logged, and stored with full metadata (see Section 3).
- **Anti-caching measures** must be in place to prevent re-use of previous outputs.
- Temperature settings must be standardized across runs (e.g., temperature = 0.2 for measurement baseline).

4.2.1 Model Version Locking

Results must reference a specific model version or snapshot.

- Example: gpt-5.0-2025-10-01
- Measurements must be **version-locked** for reproducibility.
- If the model updates, new baseline measurement must be established.

4.3 Uncertainty & Statistical Guardrails

All visibility results must include **uncertainty measures** to make scores transparent and defensible.

4.3.1 Confidence Intervals

For each cluster, calculate the 95% confidence interval:

$$CI95 = 1.96 * (\sigma / \sqrt{n})$$

Where:

- σ = standard deviation of visibility scores across prompts in the cluster
- n = number of prompts

AIVO visibility results must meet:

- Confidence interval (CI95) ≤ 5% of mean visibility score.
- Coefficient of Variation (CV) ≤ 0.10.
- Intra-class Correlation Coefficient (ICC) ≥ 0.80.

4.3.2 Coefficient of Variation

$$CV = \sigma / \mu$$

Where:

- σ = standard deviation
- μ = mean visibility score

This ensures stability of measurement within clusters.

4.4 Reproducibility Testing

DIVM requires that all visibility measurements be **independently reproducible** by a qualified third party using the same prompt set and model version.

4.4.1 Reproducibility Tolerance

$$| Score\_original - Score\_replicated | / Score\_original \leq 0.05$$

- Maximum tolerated deviation: ±5% between original and replicated runs.
- Reproducibility must be demonstrated on at least 90% of cluster prompts.

4.4.2 Rerun Protocol

- Use identical prompt set, model, and temperature.
- Reruns must occur **within the same model version window**.
- If deviation exceeds tolerance, outputs must be flagged and investigated (e.g., model instability, prompt ambiguity).

4.5 Drift, Fragility & Decay Modelling

Measurement is not static — visibility positions change as models and citations evolve. DIVM embeds **drift and fragility modelling** into its measurement standards to maintain trust over time.

4.5.1 Drift Measurement

DriftRate = (Σ |Rank_t0 - Rank_tn|) / N

Where:

- Rank_t0 = original rank
- Rank_tn = rank at time n
- N = number of prompts
- DriftRate ≥ 0.20 triggers investigation.
- DriftRate ≥ 0.35 triggers proactive decay mitigation.

4.5.2 Fragility Index

FragilityIndex = (Tier3Weight / TotalWeight) * DriftRate

Where:

- Tier3Weight = total weight of Tier 3 citations in slot
- TotalWeight = total weight of all citations

High fragility = high risk of slot collapse under competitive pressure or model updates.

4.6 Decay Curve Estimation

DIVM supports early warning of slot collapse through decay curve modelling.

$$\text{DecayRate} = (\text{Visibility\_t0} - \text{Visibility\_tn}) / \text{Visibility\_t0}$$

Where:

- Visibility_t0 = initial cluster visibility score
- Visibility_tn = score after n days

Decay curve can be plotted to forecast expected collapse dates and allocate defensive action.

- DecayRate ≥ 0.15 over 30 days = Warning threshold
- DecayRate ≥ 0.25 over 30 days = High-risk slot

4.7 Sampling Documentation & Disclosure

Every measurement report must include a **sampling appendix** documenting:

- Prompt cluster composition (categories, counts, regions).
- Model version and parameters.
- Sampling dates and cadence.
- CI, CV, and ICC values.
- Drift and fragility statistics.
- Known limitations and uncertainty disclosures.

This creates a **transparent measurement paper trail** suitable for:

- Internal governance
- Third-party audit
- Regulatory or investor reporting

4.8 Summary of Measurement Standards

Component	Requirement	Threshold
Cluster Size	Minimum 25 prompts (50 recommended)	Scale by scope
CI95	≤ 5% of mean	Statistical tolerance
CV	≤ 0.10	Stability
ICC	≥ 0.80	Reproducibility
Reproducibility	Max deviation ±5%	90% of prompts
Drift	Warning ≥ 0.20	High ≥ 0.35
Decay	Warning ≥ 0.15	High ≥ 0.25

5. Data Governance, Security & Compliance

Strong data governance is what transforms technically robust visibility measurements into **defensible, legally compliant, and enterprise-grade evidence**.

DIVM embeds security, privacy, and compliance principles directly into the data lifecycle — from collection and storage to disclosure and third-party verification. This ensures that AIVO visibility data can be trusted in boardrooms, audits, and regulatory processes globally.

5.1 Privacy & DPIA Alignment

Even though AIVO does not typically process personal data, enterprises must be able to demonstrate **compliance with privacy regulations** such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Lei Geral de Proteção de Dados (LGPD), and other global frameworks.

5.1.1 Data Minimization

- DIVM strictly prohibits the collection or storage of personally identifiable information (PII) during visibility measurements.
- Only prompt text, model metadata, and AI responses are recorded.

5.1.2 Lawful Basis & Transparency

- All data collection is purpose-bound to AI visibility measurement.
- Metadata and provenance logs are structured to support “right to explanation” and “right to audit” requests.

5.1.3 DPIA (Data Protection Impact Assessment) Templates

- DIVM includes standardized DPIA templates aligned to GDPR Article 35 and similar requirements in other jurisdictions.
- Enterprises can use these templates to demonstrate compliance and minimize internal legal workload.

5.2 Security Controls

DIVM is aligned with ISO/IEC 27001 and ISO/IEC 27701 standards for information security and privacy information management.

5.2.1 Access Control

- All data access must be role-based and logged.
- Administrative access must use MFA and be auditable.
- API keys must be rotated regularly and stored securely.

5.2.2 Encryption & Storage

- Data must be encrypted at rest (AES-256 minimum) and in transit (TLS 1.2+).
- Provenance logs must be stored on immutable or append-only infrastructure (e.g., tamper-evident logs or ledger systems).

5.2.3 Vulnerability Reporting (EU CRA Alignment)

- If DIVM or its components are classified as “digital elements” under EU Cyber Resilience Act, security incidents must be reported to relevant CSIRTs within 24 hours.
- DIVM includes an optional vulnerability reporting hook and playbook to enable rapid escalation and compliance.

5.2.4 Incident Logging & Forensics

- Every security event must be timestamped, categorized, and stored for a minimum of 24 months.
- Logs must be cryptographically linked to prevent tampering.

5.3 Data Portability & Switching

DIVM is designed to comply with portability obligations under EU Data Act (effective 2026) and related interoperability rules.

5.3.1 Standardized Export Formats

- All visibility data must be exportable in machine-readable formats (JSON and CSV as a minimum).
- Exports must include **full provenance**: prompt text, model version, timestamp, tiering, and hash values.

5.3.2 Switching Pathways

- DIVM supports seamless **data migration between vendors**, enabling enterprises to retain their historical visibility intelligence.
- This prevents vendor lock-in and strengthens procurement compliance.

5.3.3 Third-Party Verification Readiness

- Export formats are designed to be easily ingested by **independent assurance partners**, supporting external audits or regulatory reviews.

5.4 Audit & Certification Readiness

DIVM is architected to support independent assurance and certification.

Standard / Framework	Alignment
ISO 8000	Data quality
ISO/IEC 5259	Data quality for ML
ISO/IEC 27001	Security controls
ISO/IEC 27701	Privacy
ISO/IEC 42001	AI management
ISO/IEC Guide 98-3	Uncertainty of measurement
EU Artificial Intelligence Act	Governance readiness
Colorado Artificial Intelligence Act	Risk and impact documentation

5.4.1 Evidence Pack Requirements

DIVM requires that all measurement cycles produce an **evidence pack** that includes:

- Metadata logs and provenance chains.
- Statistical reproducibility outputs (CI, CV, ICC).
- Drift and fragility metrics.
- Audit log extracts.
- Security incident reports (if applicable).

5.4.2 External Assurance Compatibility

- Evidence packs are structured so they can be assessed by **independent assurance providers** such as KPMG, PwC, TÜV SÜD, or accredited data labs.
- This creates a **KPMG-layer trust model** for visibility reporting.

5.5 Governance Structures

5.5.1 Internal Governance

- Each enterprise should assign an **AIVO Data Steward** responsible for:
  - Oversight of prompt collection and measurement cycles.
  - Verification of data integrity and compliance.
  - Coordination with legal, security, and ESG teams.

5.5.2 Escalation Procedures

- DIVM requires defined escalation pathways for:
  - Security incidents,
  - Material drift or fragility events, and
  - Reproducibility failures beyond tolerance thresholds.

5.5.3 Board & Regulatory Reporting

- Governance reports should be prepared in a format suitable for:
  - Board risk committees,
  - ESG disclosures,
  - AI Act documentation, and
  - Investor relations.

5.6 Summary of Governance & Compliance Requirements

Area	Requirement	Outcome
Privacy	Non-PII, DPIA templates	GDPR/CCPA alignment
Security	Encryption, access control, CRA hooks	Protected and auditable
Portability	Structured export formats	Interoperable, verifiable
Audit	Evidence pack + third-party assurance	Regulatory readiness
Governance	Defined roles, escalation, reporting	Enterprise accountability

6. Transparency & Verification

True trust in data doesn't come from marketing claims — it comes from the ability to **prove**.
DIVM is built so that any enterprise, regulator, or assurance partner can **independently verify AI visibility results** using the same prompt set, model version, and structured evidence trail.

This transparency layer is what elevates AIVO from a "dashboard" to a **governance-grade standard**.

6.1 Replay Harness

The **Replay Harness** is a standardized mechanism that allows external parties to re-run prompt sets and verify results against the original measurements.

6.1.1 Core Requirements

- All prompt sets and metadata must be stored in a **replayable format** (e.g., JSON/CSV with full provenance fields as defined in Section 3).
- The original **model version** and **temperature settings** must be logged and disclosed.
- Replay can be executed by:
    - Third-party assurance firms,
    - Regulators,
    - Enterprise compliance teams, or
    - Independent researchers under NDA.

6.1.2 Replay Tolerance

A replay is considered valid if:

$$| \text{Score\_original} - \text{Score\_replay} | / \text{Score\_original} \leq 0.05$$

- Max tolerated deviation: ±5% per cluster.
- ≥ 90% of prompts must reproduce within tolerance.
- Drift exceptions must be documented in replay reports.

6.1.3 Replay Integrity Controls

- Prompt files must include a **hash of the original content** to detect tampering.
- Model version used must match the one in the original measurement log.
- If the model version is no longer accessible (e.g., model deprecation), results must be archived and labeled as **non-replayable** with a validity note.

6.2 Third-Party Assurance Framework

6.2.1 Purpose

DIVM is designed to support **independent assurance and certification**, creating a verifiable “KPMG layer” between AIVO data and enterprise governance.

6.2.2 Assurance Scope

Assurance providers may verify:

- Prompt set integrity
- Measurement reproducibility
- Confidence interval calculations
- Tiering and weighting logic
- Drift and fragility modelling
- Security and governance controls

6.2.3 Verification Protocol

- Access to sealed prompt sets and provenance logs.
- Independent replay using the Replay Harness.
- Replication of statistical calculations (CI, CV, ICC).
- Issuance of signed assurance statement.

6.2.4 Acceptable Deviation

- Reproducibility tolerance: ±5%
- CI and CV calculations must match original results.
- Any discrepancies must be disclosed with explanation (e.g., model version drift, provider outage).

6.2.5 Qualified Assurance Providers

Preferred assurance partners may include:

- **Big Four audit firms** (e.g., KPMG, PwC).
- Accredited digital assurance bodies (e.g., TÜV SÜD).
- Certified academic research labs.
- National regulatory bodies or designated technical services.

6.3 Disclosure & Reporting Standards

Transparency isn't optional — it's built into the methodology.
Every enterprise using DIVM for reporting must include a **minimum disclosure set** in its visibility outputs.

6.3.1 Required Disclosure Fields

Field	Description
Date of measurement	Timestamp and timezone
Model name & version	Full identifier (e.g., gpt-5.0-2025-10-01)
Prompt cluster size	Number of prompts
Prompt categories	Intent, Conversational, Transactional, etc.
Statistical summary	CI, CV, ICC
Drift / decay indicators	Fragility Index, Drift Rate, Decay Rate
Tier distribution	% of Tier 1, 2, 3 citations
Replayability status	Yes / No
Last refresh date	Most recent prompt rerun
Assurance status	None / In-progress / Third-party verified

This disclosure enables **regulators, boards, and investors** to assess the **quality and durability** of the reported visibility.

6.4 Transparency Levels

DIVM defines **three transparency levels**, allowing enterprises to choose their disclosure depth based on regulatory context or strategic posture.

Level	Description	Typical Use Case
Level 1 — Internal Audit	Internal governance, risk, ESG	Private enterprises
Level 2 — Verified Disclosure	Third-party verified reports	PLCs, regulated industries
Level 3 — Public Transparency	Full publication of prompt and metadata	High-trust or open reporting programs

6.5 Trust Seals & Verification Badges

To signal verification maturity to external stakeholders, DIVM supports a **trust seal system**:

- **DIVM Verified** — Standard replay and verification passed.
- **DIVM Assured** — Independent third-party assurance issued.
- **DIVM Public Transparency** — Full data disclosure published.

Trust seals may be displayed in ESG reports, procurement RFP responses, investor decks, or platform integrations.

6.6 Handling Non-Replayable Data

LLMs evolve, and older model versions may eventually become inaccessible. DIVM provides guidance to **maintain integrity in these cases**:

- All measurements are **timestamped** with model version and hash at collection.
- If model is deprecated:
    - Data is locked as **archival**.
    - Replayability status is set to “No.”
    - A validity note must be attached to the report.
- If an updated model produces materially different outputs, a **new baseline** must be established.

This maintains integrity even when replay is no longer technically possible.

6.7 Reporting to Regulators and Boards

Enterprises can use DIVM outputs as evidence in:

- ESG / AI Governance disclosures
- EU Artificial Intelligence Act compliance documentation
- Risk committee reporting
- Investor and analyst briefings
- Competitive visibility audits

Reports should follow a **standardized format**:

- Executive Summary (headline metrics, decay/fragility status)
- Measurement Methodology (sampling, model, CI)
- Disclosure Fields (Section 6.3)
- Assurance Statement (if applicable)
- Appendix (prompt cluster & metadata hashes)

6.8 Summary of Transparency & Verification Requirements

Area	Requirement	Tolerance / Standard
Replay Harness	Required for all prompt sets	±5% tolerance
Third-Party Assurance	Optional but recommended for PLCs	Structured protocol
Disclosure Fields	Mandatory minimum set	Section 6.3
Transparency Levels	3 tiers	Internal → Public
Trust Seals	Optional signalling layer	Verified / Assured
Non-Replayable Data	Archived + validity note	Compliance safe

7. Implementation & Operationalization

DIVM is designed to be more than a technical specification — it is a **repeatable operational framework**.
This section defines how organizations integrate DIVM into day-to-day visibility measurement, governance oversight, and reporting, ensuring that every data point is **trustworthy, auditable, and strategically actionable**.

7.1 Integration with AIVO Metrics (PSOS, QSCR, Decay)

DIVM underpins the entire AIVO Standard measurement ecosystem, ensuring that core metrics are built on **verifiable data**:

Metric	Description	DIVM Role
PSOS (Prompt-Space Occupancy Score)	Measures visibility share across prompt clusters	Ensures prompt sets, CI, and reproducibility meet standard
QSCR (Quantum Slot Collapse Risk)	Quantifies fragility and collapse probability of slots	Provides decay & drift evidence
Decay & Fragility Index	Tracks time-based vulnerability of visibility positions	Requires freshness & drift monitoring
Tier-Weighted Trust Score	Weights source tiers by reliability	Standardized tier structure and calculation

All derived metrics are **invalid** unless the underlying data complies with DIVM Sections 3–6. This ensures a consistent and defensible data foundation across all AIVO outputs.

7.2 Implementation Framework

DIVM implementation follows a **structured lifecycle** that aligns with enterprise governance processes:

7.2.1 Planning & Setup

- Define scope (brands, geographies, languages, prompt clusters).
- Establish governance roles (Data Steward, Compliance Lead, Assurance Partner).
- Configure model versioning and temperature settings.
- Set cadence for data collection and decay monitoring.

7.2.2 Data Collection

- Execute live LLM interrogations (Section 3 standards).
- Store provenance and metadata with cryptographic hashes.
- Apply tiering and trust weighting.

7.2.3 Measurement & Analysis

- Calculate PSOS, QSCR, drift, fragility, and decay metrics.
- Validate CI, CV, ICC thresholds.
- Flag anomalies or weak confidence intervals.

7.2.4 Assurance & Replay

- Package prompt sets and logs for internal or external replay.
- Trigger third-party assurance (if required).
- Document any model version changes impacting reproducibility.

7.2.5 Reporting & Disclosure

- Generate standard disclosure pack (Section 6).
- Align with AI governance, ESG, or regulatory reporting timelines.
- Publish transparency statements or trust seals where appropriate.

7.3 DIVM Compliance Checklist

A practical **DIVM Compliance Checklist** ensures enterprises meet baseline standards in every measurement cycle:

Category	Control	Requirement	Verified
Data Collection	Live interrogation	100% API call provenance	☐
Metadata	Full structured logs	Prompt, model, hash, tier	☐
Reproducibility	±5% tolerance	Replay harness required	☐
CI / CV / ICC	Statistical thresholds met	CI ≤ 5%, CV ≤ 0.10, ICC ≥ 0.80	☐
Tiering	Trust weighting applied	T1/T2/T3 structure	☐
Decay Monitoring	≤ 30 days freshness	Drift alerts active	☐
Governance	Roles defined	Data Steward assigned	☐
Assurance	External or internal verification	Optional but recommended	☐
Disclosure	Minimum fields included	Section 6.3 compliance	☐

This checklist is intended to be used by compliance officers, ESG teams, procurement leads, and assurance partners.

7.4 Versioning & Change Management

Visibility measurement is sensitive to **model changes**, prompt evolution, and regulatory updates.
DIVM includes **versioning controls** to maintain the validity of data over time.

7.4.1 Model Versioning

- Every visibility cycle must record the exact model version and snapshot.
- If the model changes, results must be re-baselined.
- Non-replayable data must be clearly labeled as **archived**.

7.4.2 Methodology Updates

- DIVM version numbers must be referenced in every report.
- Major methodology revisions require notification to assurance partners and regulatory bodies (where applicable).

7.4.3 Prompt Set Evolution

- If prompt clusters change materially, a new baseline must be established.
- Historical results must remain archived and intact.

7.5 Integration with Enterprise Governance

DIVM is designed to **plug directly into existing enterprise governance structures**, rather than requiring standalone systems.

Function	Integration Point	Example
Risk & Compliance	AI Act compliance register	QSCR and fragility risk integration
ESG / AI Governance	ESG disclosures	Visibility + assurance badges
Internal Audit	SOC / ISO audits	Replay harness and evidence packs
Investor Relations	PLC reporting	Tiered trust disclosures
Procurement	RFP / RFI due diligence	DIVM trust seals and metrics

This integration ensures AIVO visibility metrics are treated with the **same governance weight as financial and ESG disclosures**.

7.6 Operational Roles & Responsibilities

7.6.1 AIVO Data Steward

- Oversees measurement cycles.
- Ensures metadata completeness and reproducibility.
- Coordinates internal replay testing.

7.6.2 Compliance Lead

- Ensures regulatory alignment.
- Oversees DPIA and AI governance reporting.
- Manages escalation of fragility or data drift events.

7.6.3 Assurance Partner

- Verifies reproducibility and compliance with DIVM standards.
- Issues assurance statements or audit reports.

7.6.4 Executive Stakeholders

- Use verified AIVO metrics for strategic planning, investor reporting, and board risk governance.

7.7 Automation Pathways

Enterprises may automate aspects of DIVM for efficiency and accuracy:

- **Automated refresh scheduling** (e.g., 30-day cadence per prompt cluster).
- **Real-time drift monitoring** with alert thresholds.
- **Continuous replay checks** on critical prompts.
- **API-based disclosure reporting** to ESG dashboards or regulatory portals.
- **Integration with audit platforms** for automated evidence pack generation.

Automation is optional but strongly recommended for PLC-scale deployments.

7.8 Escalation & Exception Handling

Even with strong governance, issues can arise. DIVM includes structured escalation paths.

Trigger Events

- Reproducibility deviation > 5%.
- DriftRate ≥ 0.35.
- DecayRate ≥ 0.25.
- Security incident or metadata integrity breach.

Escalation Path

1. **Internal review** by Data Steward.
2. **Technical rerun** to confirm issue.
3. **Escalation to Compliance Lead**.
4. Optional **external assurance partner involvement**.
5. **Disclosure of exception** in regulatory or board reporting if material.

7.9 Implementation Timeline (Recommended)

Phase	Duration	Milestones
Phase 1 — Foundation	Month 1	Governance roles, replay harness, model lock
Phase 2 — Data Collection	Month 2	Prompt cluster execution and logging
Phase 3 — Measurement	Month 3	PSOS/QSCR calculations and drift baseline
Phase 4 — Assurance	Month 4	Internal replay verification
Phase 5 — Reporting	Month 5	First ESG / regulatory disclosure
Phase 6 — Optimization	Ongoing	Automation, Tier 1 signal reinforcement

7.10 Summary of Implementation Requirements

Area	Requirement	Benefit
Integration	DIVM must anchor all AIVO metrics	Trusted data foundation
Governance	Clear roles and escalation	Risk accountability
Versioning	Model, prompt, methodology tracking	Replay integrity
Automation	Optional but recommended	Efficiency & scale
Reporting	Standard disclosure pack	Regulatory confidence

8. Appendix

8.1 Glossary of Core Terms

Term	Definition
AIVO	AIVO Standard — The global standard and governance framework for AI Visibility measurement, assurance, and reporting.
DIVM	AIVO Data Integrity & Verification Methodology — the data standard ensuring reproducibility, transparency, and trust in AI visibility metrics.
PSOS	Prompt-Space Occupancy Score — measures the percentage of prompt clusters in which a brand holds a visibility slot.
QSCR	Quantum Slot Collapse Risk — metric estimating the probability of sudden disappearance of an AI visibility slot due to competition or model drift.
Decay Rate	Rate at which a visibility position weakens over time.
Drift Rate	Measure of how much prompt rankings or answers change over a period.
Fragility Index	Composite indicator based on tier weighting and drift that predicts slot instability.
Tiering	Classification of source citations (Tier 1–3) by trust and structure level.
Replay Harness	Mechanism for rerunning prompt sets to verify results within defined tolerance.
CI (Confidence Interval)	Statistical measure indicating reliability of the sample mean.
CV (Coefficient of Variation)	Measure of relative variability in cluster results.
ICC (Intra-class Correlation Coefficient)	Statistical metric of reproducibility across runs.
Evidence Pack	Standard bundle of metadata, calculations, logs, and disclosures used for third-party verification.
Transparency Level	Disclosure depth (Level 1 = internal, Level 2 = third-party verified, Level 3 = public).
Trust Seal	Assurance badge indicating verification maturity.

8.2 Example Metadata Schema

Below is an example JSON structure for storing DIVM-compliant provenance and metadata for a single prompt interrogation:


```
{
  "prompt_id": "8a9f1234-5678-90ab-cdef-1234567890ab",
  "prompt_text": "What are the best hotel chains in Europe?",
  "model_name": "gpt-5.0",
  "model_version": "2025-10-01",
  "temperature": 0.2,
  "timestamp_utc": "2025-10-22T15:30:45Z",
  "locale": "en-GB",
  "response_text": "The top hotel chains include Marriott, Hilton, and Accor...",
  "citations": ["wikipedia.org", "marriott.com", "hilton.com"],
  "source_tiers": ["Tier 1", "Tier 1", "Tier 1"],
  "weighted_visibility_score": 0.87,
  "response_hash": "d7e3a4b5c6d7e8f9...",
  "signature": "optional-digital-signature"
}
```


This structure can be stored in a secure data lake, replayed, and independently audited.

8.3 Regulatory Timeline (2025–2027)

Year	Regulation	Key Requirements	DIVM Alignment
2025	General Data Protection Regulation (GDPR)	Data minimization, transparency	Non-PII, DPIA templates
2025	California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)	Disclosure and opt-out rights	Provenance metadata
2026	EU Artificial Intelligence Act	Record-keeping, human oversight, risk management	Replay, DPIA, audit trail
2026	Colorado Artificial Intelligence Act	Bias & risk assessment	Replay logs, assurance
2026	EU Cyber Resilience Act	Vulnerability reporting	CRA hook and playbook
2026	EU Data Act	Portability and interoperability	Structured exports
2027	Anticipated U.S. federal AI law (TBC)	Baseline governance	Compatible with NIST AI RMF

8.4 Verification Report Template

Below is the recommended structure for **third-party assurance reports** on AIVO DIVM data.

Verification Report – AIVO DIVM Data Integrity

Issued by: [Assurance Partner]
Date: [YYYY-MM-DD]
Report ID: [Unique ID]
Verification Level: DIVM Verified / DIVM Assured

1. Scope

- Prompt clusters analyzed: [number]
- Model version: [name + date]
- Languages/locales: [list]
- Time period: [start–end]

2. Reproducibility Results

- Original PSOS: [value]
- Replay PSOS: [value]
- Deviation: [value]%
- Within ±5% tolerance: Yes/No

3. Statistical Integrity

- CI95: [value]
- CV: [value]
- ICC: [value]
- DriftRate: [value]
- DecayRate: [value]

4. Tiering & Provenance

- Tier 1 weight: [value]
- Tier 2 weight: [value]
- Tier 3 weight: [value]

- Replayable: Yes/No

5. Findings

- Data integrity breaches: [none/description]
- Model drift impact: [none/description]
- Governance observations: [notes]

6. Assurance Statement

Based on the procedures performed and evidence obtained, we conclude that the visibility results produced under DIVM meet the reproducibility and data integrity criteria defined in Sections 3–6 of the AIVO Standard.

Signature: _____
Name / Title: _____
Organization: _____

8.5 Regulatory & Standards Crosswalk

DIVM Section	Regulation / Standard	Alignment
2	GDPR / CCPA / AI Act / Data Act	Legal compliance
3	ISO 8000 / ISO/IEC 5259	Data quality
4	ISO/IEC Guide 98-3	Uncertainty of measurement
5	ISO/IEC 27001 / ISO/IEC 27701	Security and privacy
6	AI Act / NIST AI RMF	Replay, auditability
7	ESG frameworks, procurement	Operational integration
8	All	Cross-reference index

8.6 Example Fragility & Drift Calculation

Example:

- Tier 3 weight = 0.60
- Total weight = 1.00
- DriftRate = 0.25

FragilityIndex = (Tier3Weight / TotalWeight) * DriftRate
FragilityIndex = (0.60 / 1.00) * 0.25
FragilityIndex = 0.15

- Threshold:
  - Warning ≥ 0.15
  - High Risk ≥ 0.25

This slot would be flagged as **warning** and monitored in the next measurement cycle.

8.7 Example Replay Log Extract


```
{
  "prompt_id": "e1f2a345-b678-4cde-9101-112233445566",
  "prompt_text": "Best enterprise CRM software 2025",
  "model_name": "gpt-5.0",
  "model_version": "2025-10-01",
  "timestamp_utc": "2025-11-01T14:22:10Z",
  "replay_timestamp_utc": "2025-11-03T14:22:10Z",
  "original_psos": 0.68,
  "replay_psos": 0.70,
  "deviation": 0.029,
  "within_tolerance": true,
  "hash_match": true
}
```


This illustrates how replay metadata is logged and verified.

8.8 Sample Transparency Disclosure Table

Field	Value
Measurement Date	2025-10-22
Model	gpt-5.0 (2025-10-01)
Prompt Cluster	125
CI95	4.2%
CV	0.09
ICC	0.82
DriftRate	0.21
DecayRate	0.18
Tier 1 Weight	0.64
Replayable	Yes
Assurance	Third-party verified

This table can be appended to ESG reports, investor communications, or regulatory disclosures.

8.9 Recommended Escalation Thresholds

Trigger	Threshold	Action
Reproducibility deviation	> 5%	Technical rerun, assurance review
DriftRate	≥ 0.35	Escalate to compliance
DecayRate	≥ 0.25	Re-baseline
Security incident	Any	Incident playbook
Model deprecation	Any	Archive and label data

8.10 Contact & Certification Framework

Enterprises seeking to certify compliance with DIVM can engage **accredited assurance partners** for external verification.
AIVO maintains a registry of:

- Certified Replay Partners (CRPs)
- Certified Assurance Partners (CAPs)
- Public Transparency Registrants (PTRs)

Certification tiers correspond to DIVM trust seals (Verified / Assured / Public Transparency).

8.11 Formal Reference List

This reference list includes the core **regulations, ISO standards, and governance frameworks** that underpin the DIVM methodology. These references ensure alignment with global best practices, regulatory obligations, and assurance pathways.

A. Privacy & Data Protection Regulations

- General Data Protection Regulation (Regulation (EU) 2016/679)
- California Consumer Privacy Act (CCPA, 2018)
- California Privacy Rights Act (CPRA, 2020)
- Lei Geral de Proteção de Dados (LGPD, Brazil, 2018)
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada, 2000)
- Act on the Protection of Personal Information (APPI, Japan)
- Privacy Act 1988 (Australia, as amended)
- Personal Data Protection Act (Singapore, PDPA)
- EU-U.S. Data Privacy Framework (2023)

B. AI Governance & Risk Regulations

- EU Artificial Intelligence Act (Regulation (EU) — entering into force 2026)
- Colorado Artificial Intelligence Act (United States, entering into force June 2026)
- OECD AI Principles (2019)
- National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF 1.0, 2023)

C. Cybersecurity & Data Governance

- EU Cyber Resilience Act (CRA, entering into force 2026)
- EU Data Act (Regulation (EU), entering into force 2026)

D. ISO and Related Standards

- ISO 8000 — Data Quality
- ISO/IEC 5259 — Data Quality for Analytics and Machine Learning
- ISO/IEC 27001 — Information Security Management Systems
- ISO/IEC 27701 — Privacy Information Management
- ISO/IEC 42001 — AI Management Systems
- ISO/IEC Guide 98-3 — Uncertainty of Measurement (GUM)
- ISO 3534 — Statistics Vocabulary

E. Transparency & Provenance Frameworks

- W3C PROV — Provenance Interchange Standard
- “Datasheets for Datasets” (Gebru et al., 2018)
- “Model Cards for Model Reporting” (Mitchell et al., 2019)

8.12 Standards Mapping Annex

This annex maps **DIVM sections** to **specific regulatory and ISO references** to support **procurement due diligence**, **regulatory submissions**, and **third-party assurance**.

DIVM Section	Regulation / Standard	Clause / Article	Alignment Summary
§2 Legal & Regulatory Alignment	GDPR	Articles 5, 30, 35	Data minimization, processing records, DPIA
§2 Legal & Regulatory Alignment	CCPA/CPRA	Sec. 1798.100–1798.199	Consumer rights, data transparency
§2 Legal & Regulatory Alignment	EU AI Act	Arts. 9, 10, 12, 52	Risk management, data governance, record keeping
§2 Legal & Regulatory Alignment	Colorado AI Act	Sec. 6-1-1703	Risk and bias assessment
§2 Legal & Regulatory Alignment	EU CRA	Art. 11–14	Vulnerability reporting
§2 Legal & Regulatory Alignment	EU Data Act	Art. 4–8	Portability & interoperability
§3 Data Integrity Framework	ISO 8000	Data quality principles	Accuracy, completeness, traceability
§3 Data Integrity Framework	ISO/IEC 5259	ML data quality	Provenance, structured metadata
§3 Data Integrity Framework	W3C PROV	Core provenance model	Chain of custody
§4 Measurement & Reproducibility	ISO/IEC Guide 98-3	Measurement uncertainty	Confidence intervals
§4 Measurement & Reproducibility	ISO 3534	Statistical terminology	Standardized calculation
§5 Governance, Security & Compliance	ISO/IEC 27001	A.5–A.18	Information security controls
§5 Governance, Security & Compliance	ISO/IEC 27701	PIMS Clauses 5–8	Privacy management

§6 Transparency & Verification	EU AI Act	Arts. 12, 52	Transparency and record access
§6 Transparency & Verification	NIST AI RMF	Map, Measure, Manage	Risk and reproducibility
§7 Implementation	ESG Frameworks	GRI / CSRD references	Sustainability reporting
§8 Appendix	All	—	Reference consolidation

Note: This annex is maintained as a **living table**. As regulatory frameworks evolve (e.g., U.S. federal AI legislation, EU AI Liability Directive), future DIVM versions will update alignment references accordingly.