Algorithmic Coordination Diagnostic (ACD)

Product Specification

September 2025

1. Executive Summary

The Algorithmic Coordination Diagnostic (ACD) is an agent-driven monitoring platform designed to detect, explain, and report algorithmic coordination risks in real-time across the most coordination-prone industries. It combines econometric rigor with natural-language reporting to make complex statistical diagnostics accessible to compliance teams, regulators, litigators, and courts.

Problem: Airlines, financial institutions, telecommunications companies, and e-commerce platforms increasingly rely on sophisticated pricing algorithms—from revenue management systems and reinforcement learning models to price-matching algorithms and ensemble methods. These systems can inadvertently create coordination patterns that violate competition law, even when designed for legitimate competitive purposes. Traditional economic analysis takes months and costs hundreds of thousands of dollars, leaving companies vulnerable during investigations and unable to proactively assess coordination risks.

Solution: ACD applies novel dual-pillar econometric methodology — Invariant Causal Prediction (ICP) and Variational Method of Moments (VMM) — to distinguish competitive adaptation from coordination across different algorithm types. The system builds expertise by analyzing client-submitted algorithms and independently monitoring market pricing patterns. An intelligent agent translates rigorous statistical findings into court-ready evidence and natural-language explanations accessible to non-economists.

Core Differentiator: ACD combines cutting-edge causal inference methodology with practical accessibility and industry-specific algorithm classification. The statistical engine detects coordination through environment sensitivity analysis across 14 distinct algorithm categories — from simple price-matching rules to complex multi-agent systems — while the agent interface provides immediate, actionable insights for compliance teams, regulators, and courts. Unlike traditional consultancies, ACD delivers analysis in hours rather than months at a fraction of traditional costs.

Target Market: Airlines using revenue management systems, financial institutions deploying ML-based pricing, telecommunications companies with game-theoretic pricing models, e-commerce platforms using ensemble pricing methods, and the legal/regulatory bodies that oversee them.

Commercial Model: Enterprise SaaS subscriptions ($500k–$2m/year) with industry-specific pricing tiers, litigation support packages for active investigations, and regulatory licensing for competition authorities seeking systematic algorithmic coordination detection tools.

2. Methodological Foundations

ACD is anchored in RBB Brief 55+, which established the methodological basis for algorithmic coordination detection. The platform operationalizes these methods:

Invariant Causal Prediction (ICP): Detects whether structural relationships between firm prices and market environments remain stable (competitive) or become invariant across environments (collusive).

Variational Method of Moments (VMM): Provides continuous monitoring by fitting dynamic moment conditions to observed price/market data, identifying structural deterioration in real-time.

Dual Pillars

Pillar 1: Invariant Causal Prediction (ICP)

- Formal statistical framework
- Tests for stability vs invariance of causal relationships
- Multi-environment robustness

Pillar 2: Variational Method of Moments (VMM)

- Adaptation of financial risk monitoring
- Online, streaming estimation
- Sensitive to subtle coordination signals in large datasets

Together, ICP and VMM form a redundant, complementary detection framework: ICP provides hypothesis-driven statistical guarantees, while VMM enables high-frequency monitoring and adaptive learning.

3. Econometric Specifications

3.1 Invariant Causal Prediction (ICP)

Given:

- A set of environments $e \in \mathcal{E}$ (e.g., demand regimes, cost shocks, time periods)
- Price vector P, explanatory variables X, environment label E

We estimate structural models:

$$P = f(X) + \varepsilon$$

where ε is an error term.

Null Hypothesis: H_0: f(X) is invariant across $e \in \mathcal{E}$ **Alternative Hypothesis**: H_1: f(X) differs across some $e \in \mathcal{E}$

Test Statistic: We compute:

$$T = \max_{e \in \mathcal{E}} |\hat{f}_e(X) - \hat{f}(X)|$$

and reject H_0 if $T > c_\alpha$, where c_α is a critical value determined via bootstrap.

Parameters:

- Significance level: $\alpha = 0.05$
- Minimum samples per environment: $n \geq 1000$
- Power requirement: $1-\beta \geq 0.8$ for effect sizes $\Delta f \geq 0.2\sigma_P$

3.2 Variational Method of Moments (VMM)

We define specific moment conditions for coordination detection:

Price-cost pass-through: $m_1(Z_i, \theta) = (P_i - MC_i) - \theta_1$ **Cross-price sensitivity**: $m_2(Z_i, \theta) = \partial P_i/\partial P_j - \theta_2$ **Environment sensitivity**: $m_3(Z_i, \theta) = \partial P_i/\partial E - \theta_3$

where:

- θ_2 measures how much firm i's price responds to rival j's price (high θ_2 suggests lockstep movement)
- θ_3 measures how much firm i's price adapts to exogenous shocks (low θ_3 indicates coordination)

Coordination Index: $CI = \mathbb{E}[\theta_2] - \mathbb{E}[\theta_3]$

- High cross-price sensitivity minus low environment sensitivity → evidence of structural coordination

Objective Function:

$$\hat{\theta} = \arg\min_\theta \{ (1/n)\sum_{i=1}^n ||m(Z_i, \theta)||^2 + \lambda D_{KL}(q_\varphi(\theta)||p(\theta)) \}$$

where:

- λ: regularization coefficient (default: 0.01)
- D_KL: Kullback-Leibler divergence between variational distribution $q_\varphi(\theta)$ and prior $p(\theta)$

Convergence Criteria:

- Gradient norm $||\nabla_\phi L|| < 10^{-6}$
- Max iterations = 10,000
- Early stopping if ELBO improvement < 10^{-8} over 200 iterations

Signal Detection Thresholds:

- Red flag if CI > δ = 0.1 (default threshold)
- Red flag if moment violation exceeds 2 standard deviations across ≥ 3 consecutive monitoring windows
- Monitoring window = 5 minutes, rolling

Non-Convergence Handling: If VMM fails to converge within max iterations:

1. Flag as amber risk
2. Annotate report with: "Data quality or model instability detected; results may be inconclusive."
3. Automatic retry with adjusted hyperparameters:
    - Max iterations doubled (20,000)
    - Gradient tolerance relaxed (10^{-4})
    - Priors widened (increase variance of θ priors)
4. If unresolved for 3+ consecutive cycles: trigger data quality audit and compliance officer notification

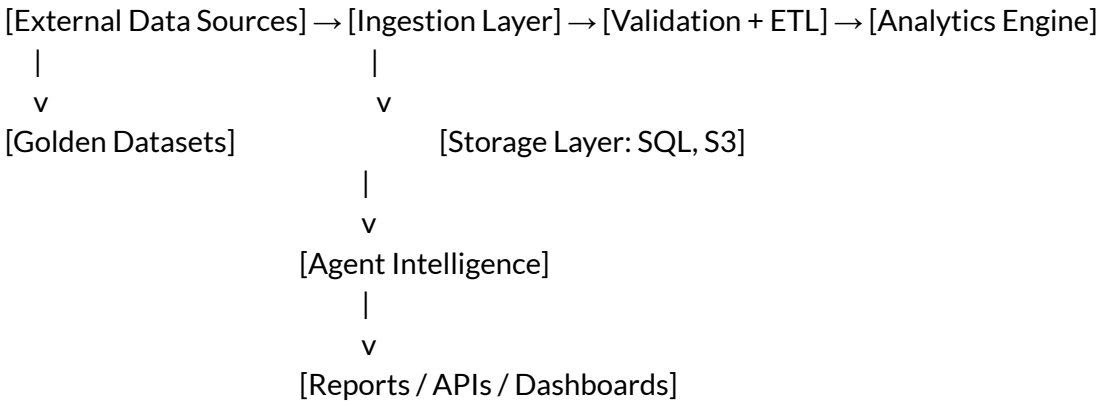
4. System Architecture

4.1 High-Level Components

- **Data Ingestion Layer**: Connectors for client feeds, market APIs, independent datasets
- **Econometric Engine**: ICP testing module + VMM online estimator
- **Agent Layer**: LLM interface generating natural-language reports
- **Audit Layer**: Cryptographic timestamping, hash-chained logs, optional external anchoring
- **Frontend**: React/TypeScript UI with dashboards, alerts, and agent chat
- **Backend**: FastAPI services orchestrating econometric computations, Redis for caching, Celery for jobs

4.2 Data Flow

The ACD platform follows a modular service-oriented architecture:



1. **Collection**: Prices, costs, demand indicators ingested in 5-min intervals
2. **Validation**: Data schemas enforced, anomalies flagged
3. **Analysis**: ICP run daily; VMM run continuously in 5-min windows
4. **Storage**: PostgreSQL for structured data, Redis for in-memory ops
5. **Reporting**: Agent composes plain-language outputs, dashboards updated
6. **Archival**: Immutable logs stored with hash + timestamp

4.3 Data Schema (Core Tables)

Table: transactions

Field	Type	Description
txn_id	UUID	Unique transaction ID
firm_id	UUID	Identifier for firm
product_id	UUID	Product/market identifier
timestamp	TIMESTAMP	Event time
price	NUMERIC	Transaction price
cost_estimate	NUMERIC	Estimated marginal cost
environment	JSONB	Encoded demand/cost/regulatory environment

Table: environment_events

Field	Type	Description
event_id	UUID	Unique event ID

type	TEXT	{demand_shock, cost_shock, regulation}
description	TEXT	Human-readable description
timestamp	TIMESTAMP	Event occurrence time

Table: risk_outputs

Field	Type	Description
run_id	UUID	Monitoring cycle ID
firm_id	UUID	Firm identifier
invariant_flag	BOOLEAN	ICP stability test outcome
coordination_index	FLOAT	VMM-derived coordination measure
risk_score	INT	Normalized 0–100 risk index
report_hash	TEXT	Audit trail reference (SHA-256 hash)
created_at	TIMESTAMP	Timestamp of result

4.4 Security Architecture

Threat Model: STRIDE

Category	Representative Threats	Mitigations
Spoofing	Credential stuffing; session hijack	OAuth2/OIDC; WebAuthn/FIDO2 optional; short-lived JWTs (≤15m) + refresh; IP reputation checks
Tampering	Payload or result manipulation	TLS 1.3; HSTS; signed requests; WAF; cryptographic signatures on outputs; write-once evidence store
Repudiation	"I didn't run that analysis"	Event-sourced logs (immutable), time-stamped actions, per-user signing keys, non-repudiation receipts
Information Disclosure	Data exfiltration (API keys, datasets)	KMS-managed envelope encryption; VPC isolation; egress proxy allow-lists; DLP scanners; field-level encryption

Denial of Service	API floods; resource exhaustion	Autoscaling; token buckets & leaky buckets; per-org quotas; circuit breakers; CDN/edge WAF
Elevation of Privilege	Horizontal/vertical privilege jumps	RBAC/ABAC with policy engine (OPA/Cedar); unit/integration authZ tests; strict tenancy guards at DB & cache layers

Access Control Matrix:

Role	**Data Access**
Analyst	Read-only on risk outputs
Compliance Officer	Full read + audit logs
Admin	Read/write on configs, limited DB write
External Regulator	Read-only, court-export only (PDF/CSV)

5. Performance Specifications

5.1 Latency Budgets

The ACD platform is engineered to support real-time monitoring of algorithmic coordination in markets with high-frequency data flows.

Stage	**Target Latency (p95)**	**Hard SLA (p99)**
Ingestion → Validation	≤ 1.0s	≤ 2.0s
Validation → Analytics Input	≤ 2.0s	≤ 3.5s
ICP/VMM Analytics Execution	≤ 3.0s	≤ 5.0s
Risk Output → Report Render	≤ 2.0s	≤ 3.0s
Total End-to-End Cycle	≤ 8.0s	≤ 12.0s

- Monitoring cycles run every 5 minutes, but the system is designed to allow sub-10 second turnaround per batch to ensure freshness
- Streaming mode supports near real-time incremental updates (<2s per event)

5.2 Throughput Targets

- **Normal load**: 50,000 datapoints/minute
- **Stress-tested load**: 250,000 datapoints/minute sustained for ≥ 60 minutes

- **Burst capacity**: 1,000,000 datapoints/minute for ≤ 5 minutes without service degradation

Scaling achieved via:

- Horizontal scaling of ingestion workers (Kubernetes HPA)
- Partitioned analytics queues across Redis and Celery
- Shard-aware ICP/VMM processing

5.3 Scalability Benchmarks

Dimension	Specification
Horizontal Scaling	Linear up to 100 ingestion workers
Vertical Scaling	Analytics nodes up to 64 cores / 512GB RAM
Multi-region Support	Active-active clusters in 3 regions (NA, EU, SA)
Load Balancing	Nginx + Envoy with sticky session routing
Data Sharding	PostgreSQL partitioning by firm_id + time

5.4 Availability & Reliability

Service Tiers (per enterprise contract):

- **Silver SLA**: 99.5% uptime, RTO 12h, RPO 6h
- **Gold SLA**: 99.9% uptime, RTO 4h, RPO 1h
- **Platinum SLA**: 99.99% uptime, RTO 30m, RPO 15m

Definitions:

- **RTO (Recovery Time Objective)**: Maximum downtime tolerated
- **RPO (Recovery Point Objective)**: Maximum data loss window tolerated

5.5 Disaster Recovery & Failover

- **Primary Strategy**: Multi-region deployment with automated failover via DNS + load balancer failover
- **Database Replication**:
    - PostgreSQL streaming replication with synchronous commit (lag < 1s)
    - Redis with Redis Sentinel automatic failover
- **Backups**:
    - Full daily snapshots (Postgres, S3 object store)
    - Incremental every 15 minutes
    - Stored across 3 separate cloud regions

- **Disaster Recovery Drills**: Mandatory quarterly simulation with <1h recovery demonstration

5.6 Degraded Mode Operations

When persistent non-convergence or data instability occurs:

- Confidence intervals widened by +50%
- Detection thresholds δ doubled (e.g., δ = 0.1 → 0.2)
- Risk classification defaults to amber unless invariance is overwhelming
- Mathematical approach reduces false positives while maintaining "innocent until proven guilty" standards

6. Risk Classification Framework

6.1 Risk Score Scale

LOW (0–33): Algorithms show environment sensitivity — price responses adapt to cost/demand shocks, consistent with competitive behavior.

- Example: Price decreases when marginal costs decrease across environments
- Treatment: Routine monitoring only

AMBER (34–66): Algorithms show borderline invariance — stability in relationships across environments that warrant further scrutiny.

- Example: Multiple firms' prices co-move across distinct demand shocks
- Treatment: Enhanced monitoring, regulator notification optional

RED (67–100): Algorithms show statistically significant invariance inconsistent with competitive adaptation.

- Example: Prices remain fixed across different cost/demand regimes
- Treatment: Trigger investigation, generate court-ready evidence

6.2 Statistical Translation

Risk score R is computed as a weighted aggregation:

$$R = w_1 \cdot \mathbb{1}(\text{ICP reject}) + w_2 \cdot \min(1, CI/\delta) + w_3 \cdot \Delta\text{Environment Sensitivity}$$

where w_1, w_2, w_3 are calibrated weights (default: 0.4, 0.4, 0.2).

Combined Risk Score:

$$R = 50 \cdot \mathbb{1}(\text{ICP rejects}) + 50 \cdot \min(1, CI/\delta)$$

7. Commercial Applications

7.1 Target Markets

Financial Institutions: Banks deploying pricing algorithms in lending or derivatives **Airlines & Transport**: Revenue management systems vulnerable to parallel pricing **Digital Platforms**: Marketplaces with dynamic pricing across multiple sellers **Legal/Compliance Teams**: Law firms and in-house counsel preparing defenses or regulatory submissions **Competition Authorities**: Antitrust and sector regulators requiring proactive monitoring tools

7.2 Use Cases

- **Enterprise Compliance**: Continuous monitoring to prevent investigations
- **Litigation Support**: Evidence generation for defense or prosecution
- **Regulatory Pilots**: Agencies deploying ACD in sandbox environments
- **Risk Management**: Early warning detection for boards and risk officers

8. Value Propositions

8.1 Proactive Compliance

Prevents regulatory surprises by flagging coordination before enforcement.

8.2 Litigation Defense

- Generates expert-testimony ready econometric evidence
- Audit trails withstand courtroom admissibility scrutiny

8.3 Regulatory Preparation

- Enables pre-investigation compliance checks
- Demonstrates "good faith" monitoring to regulators

8.4 Risk Management

Provides executive dashboards translating econometric findings into business KPIs.

9. Technology Stack

9.1 Backend

- **Framework**: Python 3.11, FastAPI

- **Data Storage**: PostgreSQL 15, Redis 6
- **Distributed Processing**: Celery with RabbitMQ
- **Analytics**: NumPy, SciPy, Statsmodels, PyTorch (for variational inference)

9.2 Frontend

- **Framework**: React 18, TypeScript
- **UI Library**: Material-UI, Tailwind CSS for responsive design
- **Charts**: D3.js, Chart.js for econometric plots
- **Agent Chat**: WebSocket + SSE streaming integration

9.3 Infrastructure

- **Orchestration**: Kubernetes on AWS/GCP
- **Containerization**: Docker, Helm
- **Logging & Monitoring**: Prometheus, Grafana, ELK stack
- **CI/CD**: GitHub Actions, Codecov, Dependabot

9.4 Security

- **Encryption**: AES-256 at rest, TLS 1.3 in transit
- **Access Control**: OAuth2.0 / JWT with RBAC
- **Compliance**: GDPR, SOX, Basel III operational risk standards

10. Implementation Roadmap

Phase 1 (Months 1–6): Pilot Validation

- Partner: FNB CDS market data
- Deliverable: Proof-of-concept showing collusion detection in financial derivatives
- Target: Validate ICP + VMM in real-world data

Phase 2 (Months 7–12): Regulatory Sandbox

- Deploy ACD in South African and EU sandboxes
- Deliverable: Full dashboards + agent reporting
- Target: Demonstrate court-ready reporting in regulatory context

Phase 3 (Year 2): Industry Compliance Programs

- Scale deployments to airlines, banks, and digital platforms
- Deliverable: Multi-client SaaS, 24/7 uptime
- Target: Monetize enterprise subscription model

Phase 4 (Year 3): Commercial Rollout

- Scale to US/EU regulators, tier-1 banks

- Deliverable: Platinum SLA, global multi-region failover
- Target: Become standard compliance tool

11. Commercial Model

11.1 Subscription Pricing

Silver ($500k/year):

- 99.5% uptime SLA
- Daily ICP testing + 5-min VMM updates
- Quarterly compliance reports
- Standard rate limits (10k req/min, burst 20k)

Gold ($1m/year):

- 99.9% uptime SLA
- Enhanced monitoring (multi-environment ICP, full VMM cycle)
- Monthly compliance reports
- Dedicated account manager
- Higher rate limits (20k req/min, burst 40k)

Platinum ($2m/year):

- 99.99% uptime SLA
- 24/7 monitoring + real-time alerting
- Court-testimony support packages
- Annual regulator workshop
- Premium rate limits (50k req/min, burst 100k)

11.2 Litigation Support

- **Case-Based Retainer**: $250k–$500k per litigation matter
- Includes dataset analysis, expert witness reports, and agent-generated evidence packages

11.3 Regulatory Licensing

- **Pilot programs**: $250k–$500k/year for competition authorities
- Includes regulator dashboards + evidence generation modules

11.4 Professional Services

- **Integration Support**: $50k–$100k per deployment
- **Custom Econometric Modules**: T&M billing at $500/hour

12. Data Strategy & Quality Management

12.1 Multi-Tier Data Acquisition

Tier 1: Direct Client Feeds

- Primary ingestion of client CDS curves, internal pricing, transaction data
- Real-time API connections with fallback mechanisms

Tier 2: Global Independent Feeds

- S&P Global / IHS Markit (~$250k+/yr enterprise)
- ICE Data Services (~$150k+/yr enterprise)
- Refinitiv CDS/bond pricing (~$100k+/yr enterprise)

Tier 3: South African Market Proxies

- JSE-listed bank bond spreads
- SARB sovereign yield curves
- National Treasury auction results

Tier 4: Derived Signals

- Bond-CDS basis modeling
- ZAR FX volatility
- Cross-currency basis spreads
- Rating agency announcements

12.2 Data Quality & Fallback Management

Cross-Validation

- Compare client vs. independent feeds, flag discrepancies > ±5bps
- Discrepancy thresholds vary by market liquidity (liquid: 3-5bps, semi-liquid: 5-10bps, illiquid: 10-20bps)

Quality Metrics:

- **Completeness**: ≥ 99% fields populated (per dataset)
- **Latency**: < 60s ingestion-to-availability SLA
- **Consistency**: All timestamps normalized to UTC+0, ISO 8601 format
- **Deduplication**: Hash-based duplicate detection at ingestion
- **Cross-validation**: Prices cross-checked against independent feeds (public + derived indices)

Confidence Scoring

- Each datapoint tagged 0-100 based on source reliability, recency, and variance vs. peers
- Weighted composite fine-tuned via historical manipulation cases

Fallback Triggers

- Auto-switch if client feed silent >10 minutes
- Manual override (requires compliance/legal authorization)
- Hysteresis: 2 consecutive healthy checks before reverting

12.3 Data Retention & Archival

- **Hot storage** (Postgres, Redis): 12 months rolling window
- **Warm storage** (S3/GCS): 7 years archive, encrypted (AES-256)
- **Immutable log**: Cryptographically hashed, retained indefinitely
- **Deletion**: GDPR-compliant right-to-be-forgotten procedure on PII

Appendix A – Mathematical Foundations

A.1 Invariant Causal Prediction (ICP) - Complete Specification

Problem Setup: Let:

- Y = outcome variable (firm price)
- X = covariates (cost drivers, demand shifters, competitor prices)
- E = environment index (market regime, time window, policy regime)

We assume a structural causal model (SCM):

$Y = f(X, \varepsilon), \varepsilon \perp E$

where f is invariant across environments.

Hypothesis Testing: For candidate subset $S \subseteq X$:

- **Null (H_0)**: $P(Y \mid X_S, E = e) = P(Y \mid X_S)\ \forall e$ (conditional distribution stable across environments)
- **Alternative (H_1)**: $\exists e_1, e_2: P(Y \mid X_S, E = e_1) \neq P(Y \mid X_S, E = e_2)$

Test Procedure:

1. Estimate predictive model $\hat{f}_S$ using regression/classification
2. Compute residuals: $\hat{\varepsilon}_{i,S} = Y_i - \hat{f}_S(X_{i,S})$
3. Test residual distribution across environments using Kolmogorov-Smirnov (KS) or Levene's test for variance

Formally:

$T_S = \max_{e_1,e_2} D_{KS}(\hat{\varepsilon}_{S,e_1}, \hat{\varepsilon}_{S,e_2})$

Reject H_0 if $T_S > c_\alpha$, where c_α is critical value at significance level α.

Parameter Specifications:

- Significance level: $\alpha = 0.05$ (default)
- Minimum sample size per environment: $n_e \geq 1000$
- Power requirement: ≥ 0.8 for effect size $\Delta \geq 0.2$ (Cohen's d)
- Environment dimensions: demand shocks, cost shocks, regulatory events

Output of ICP:

- Invariant sets: Candidate causal parents of Y
- Failure of invariance: Evidence of coordination (algorithms behaving in a stable, non-competitive way across shocks)

A.2 Variational Method of Moments (VMM) - Complete Implementation

Problem Setup: We observe data Z_i across time/environments. We want to estimate parameters θ describing algorithmic interaction.

Moment conditions: $\mathbb{E}[m(Z_i, \theta)] = 0$

Examples of moment functions $m(\cdot)$:

- Price-cost pass-through: $m_1(Z_i, \theta) = (P_i - MC_i) - \theta_1$
- Cross-price sensitivity: $m_2(Z_i, \theta) = \partial P_i/\partial P_j - \theta_2$
- Environment sensitivity: $m_3(Z_i, \theta) = \partial P_i/\partial E - \theta_3$

Variational Objective: Instead of classical GMM, we solve a variational approximation:

$\min_{q_\varphi(\theta)} \mathbb{E}_{q_\varphi(\theta)}[||(1/N)\sum_i m(Z_i, \theta)||^2] + \lambda D_{KL}(q_\varphi(\theta)||p(\theta))$

- $q_\varphi(\theta)$: variational distribution (Gaussian family)
- $p(\theta)$: prior (uninformative or Bayesian shrinkage prior)
- D_{KL}: Kullback-Leibler divergence regularizer
- λ: penalty weight

Convergence Criteria:

- Gradient norm tolerance: $||\nabla_\phi L|| < 10^{-6}$
- Max iterations: 10,000
- Early stopping if ELBO improvement $< 10^{-8}$ over 200 iterations

Statistical Properties:

- Consistency: As $N \to \infty$, estimator converges to true parameter under correct specification
- Robustness: Variational relaxation prevents overfitting small-sample noise
- Output: Distribution over coordination parameters with confidence intervals

Signal Detection Thresholds: Define coordination index:

$CI = \mathbb{E}_{q_\varphi(\theta)}[\theta_2] - \mathbb{E}_{q_\varphi(\theta)}[\theta_3]$

- If $CI \approx 0$: competitive adaptation
- If $CI > \delta$ (threshold): evidence of structural coordination
- Default threshold $\delta = 0.1$

Statistical Power & Effect Size:

- Detectable effect size: ≥ 0.2 standard deviations across environments
- Power: ≥ 0.8
- False discovery rate controlled at $q = 0.1$ using Benjamini-Hochberg

Appendix B – Security & Compliance Framework

B.1 Data Classification & Handling

Class	Examples	Storage & Transport	Access Controls	Retention
C1 – Public	Marketing docs, README	S3 standard; TLS	No auth	Indefinite
C2 – Internal	Non-production configs, telemetry	Encrypted S3; TLS	Staff SSO	12 months
C3 – Confidential	Model configs, monitoring outputs, non-PII datasets	AES-256 at rest; TLS; row-level encryption for sensitive fields	Project roles + need-to-know	24 months (configurable)
C4 – Restricted	Client source data, legal work-product, PII	AES-256 at rest + field-level encryption; hardware-backed KMS; private subnets	Client-scoped roles; dual-control for exports	90 days default (client override), 7 yrs for evidentiary artifacts

Data residency: Choose region at org provisioning (EU/NA/SA). Analytical artifacts and logs remain in-region. Cross-region DR copies use client-approved jurisdictions only.

B.2 Identity, Authentication & Authorization

- **Identity**: OAuth2/OIDC (AzureAD/Okta/Google), SCIM for user lifecycle, SAML 2.0 optional
- **AuthN**:
    - Primary: OIDC + short-lived access token (≤15 min) and refresh token (≤24 h)
    - MFA: TOTP or WebAuthn (enforced per org policy)
    - Service-to-service: mTLS + workload identity (GCP/AWS IAM)
- **AuthZ**:
    - RBAC base + ABAC constraints (tenant_id, data_domain, classification)
    - Policy engine (OPA/Cedar). Policies reviewed & tested; deny-by-default
- **Session Security**: SameSite=strict cookies for browser flows; token binding to device fingerprint (optional)
- **Secrets**: No secrets in code; sealed secrets; automatic rotation (≤90 days; ≤24 h for critical)

B.3 Multi-Tenant Isolation

- **Logical isolation**: tenant_id scoped DB partitions + RLS (Row Level Security) in Postgres
- **Cache isolation**: Redis keyspace prefix per tenant + ACLs
- **Compute isolation**: Namespaces and network policies in Kubernetes; per-tenant resource quotas
- **File isolation**: S3 buckets per tenant; KMS keys per tenant; IAM boundaries

B.4 Key Management & Cryptography

- **KMS**: AWS KMS / GCP KMS; envelope encryption for data and artifacts
- **Encryption in transit**: TLS 1.3 everywhere; HSTS; Perfect Forward Secrecy
- **Encryption at rest**: AES-256-GCM for object storage; pgcrypto for selected columns; hash-pepper for IDs used in URLs
- **Key rotation**: Automatic (≤90 days) and ad-hoc; dual control for C4 key operations; audit logs on every use

B.5 Audit Trails & Evidence Chain

Immutable Logs:

- Append-only event store (e.g., AWS QLDB or WORM S3 with object lock)
- All actions include: user/service principal, tenant_id, request hash, dataset version, model version, time, IP, policy decision, cryptographic attestation

Evidence Artifacts:

- Each report bundle contains: inputs manifest (hashes), environment config, ICP/VMM params, test statistics, p-values, charts, NLG summary, and signature
- Hash chaining: Every artifact includes SHA-256 + parent hash pointer (Merkle-style)
- External anchoring (optional, default OFF): Daily consolidated hash anchored via notary service. Clients can enable public chain anchoring (e.g., Bitcoin timestamps or independent TSA). We avoid default Ethereum mainnet anchoring to reduce operational friction

B.6 Compliance Mappings

Reg/Std	Requirement	ACD Controls
GDPR	Lawful basis; data minimization; DSAR; RTBF; DPA	Regional data residency; per-tenant KMS; export tooling; deletion SLAs; sub-processor list
SOX	Access controls; change management; audit logs	RBAC/ABAC; 4-eyes on production changes; immutable logs; CI/CD approvals; segregation of duties
Basel III/OpRisk	Resilience; model risk mgmt; auditability	Multi-region DR; model versioning; evidence chain; backtesting on golden datasets
ISO/IEC 27001	ISMS scope, risk assessments, controls	Policy set, risk register, supplier due diligence, continuous monitoring
SOC 2 (TSC)	Security, Availability, Confidentiality	SLAs, DR drills, encryption, auditability, change control, vendor management
PCI-DSS	Card data isolation	Not in scope by default; segmentation enforced if required

Appendix C – API Specifications

C.1 Overview

- **Base URL**: https://api.acd-monitor.com/v1
- **API Style**: REST + Server-Sent Events (SSE) for streaming
- **Content Types**: application/json (default), text/event-stream (SSE)
- **Auth**: OAuth2 Client Credentials (server-to-server) or PAT (scoped personal access token)
- **Idempotency**: Supported on POST/PUT with Idempotency-Key header
- **Versioning**: URI-based (/v1), additive changes only; breaking changes announced ≥90 days
- **Time**: All timestamps are RFC3339 UTC (e.g., 2025-09-11T14:08:00Z)

C.2 Authentication & Authorization

OAuth2 (Client Credentials):

- Token endpoint: POST https://auth.acd-monitor.com/oauth/token
- Grant: client_credentials
- Scopes: read:analytics, write:analytics, read:evidence, write:evidence, read:events, write:events, read:audit, admin:org (restricted)

Request:

```
curl -s -X POST https://auth.acd-monitor.com/oauth/token \
 -H "Content-Type: application/json" \
 -d '{
  "grant_type":"client_credentials",
  "client_id":"<CLIENT_ID>",
  "client_secret":"<CLIENT_SECRET>",
  "scope":"read:analytics read:evidence read:events"
 }'
```

Response:

```
{
 "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI...",
 "token_type": "Bearer",
 "expires_in": 3600,
 "scope": "read:analytics read:evidence read:events"
}
```

Personal Access Tokens (PAT):

- Created in the ACD Console by org admins
- Header: Authorization: Bearer <PAT>
- Scopes same as OAuth2

C.3 Rate Limiting & Quotas

- **Default**: 10,000 req/min/org, burst 20,000 (Silver tier)
- **Gold Tier**: 20,000 req/min/org, burst 40,000 (contractual)
- **Platinum Tier**: 50,000 req/min/org, burst 100,000 (contractual)
- **Headers returned on each request**:
    - X-RateLimit-Limit
    - X-RateLimit-Remaining
    - X-RateLimit-Reset (UTC epoch seconds)

- **429 Retry-After** header provided. Exponential backoff recommended (250ms · 2^n, jitter)

C.4 Core Endpoints

Risk Assessment:

```
GET /api/v1/risk/summary?timeframe=30d
Response:
{
 "score": 14,
 "band": "LOW",
 "confidence": 92,
 "source": {
  "freshnessSec": 45,
  "dataFeeds": ["bloomberg:fwd_cds", "client:pricing"]
 },
 "explanation": "Environment sensitivity consistent with competition",
 "request_id": "req_..."
}
```

Analytics Results:

```
GET /api/v1/analytics/icp-results?productId=nike-shoe-123
Response:
{
 "H0": "Price relationships are environment-invariant",
 "pValue": 0.02,
 "rejectH0": true,
 "effectSize": 0.15,
 "confidenceInterval": [0.08, 0.22],
 "sampleSize": 1200
}
```

```
GET /api/v1/analytics/vmm-results?productId=nike-shoe-123
Response:
{
 "objectiveValue": 123.45,
 "converged": true,
 "iterations": 350,
 "gradientNorm": 1e-7,
 "coordinationIndex": 0.12,
 "momentsMatched": ["mean", "variance", "lag1_autocorrelation"],
 "KLRegularization": 0.01
}
```

Evidence Generation:

POST /api/v1/evidence/generate
Request:
```
{
 "conversationId": "conv_12345",
 "range": {"from": "2025-09-10T00:00:00Z", "to": "2025-09-11T00:00:00Z"},
 "inclusions": ["risk_summary", "metrics", "events", "chat_context"],
 "format": "zip"
}
```

Response:
```
{
 "bundle_id": "ev_9c8b7a",
 "status": "PENDING",
 "request_id": "req_..."
}
```

Agent Chat:

POST /api/v1/agent/chat
Request:
```
{
 "conversationId": "conv_12345",
 "messages": [
  {"role": "user", "content": "Explain current risk classification"}
 ],
 "temperature": 0,
 "stream": false
}
```

Response:
```
{
 "reply": "Current risk classification is LOW (14/100) based on...",
 "usage": {"input_tokens": 812, "output_tokens": 256},
 "evidence_pointer": "ev_9c8b7a",
 "request_id": "req_..."
}
```

Data Ingestion:

POST /api/v1/ingest/prices
Request:

```
{
 "tenantId": "abc123",
 "timestamp": "2025-09-11T20:30:00Z",
 "productId": "cds-fnb-5y",
 "price": 150.5,
 "currency": "ZAR",
 "marketEnv": "SA-banking"
}
```


Response: 202 Accepted

```
{"batch_id": "batch_567", "request_id": "req_..."}
```


C.5 Webhooks

Configurable Events:

- risk.alert → Fires on RED risk classification
- evidence.ready → Fires when evidence bundle generated
- system.error → Fires on ingestion/analysis failures
- risk.classification.updated → Fires on band changes

Event Format:


```
{
 "id": "wh_01H...",
 "type": "risk.classification.updated",
 "created_at": "2025-09-11T14:05:00Z",
 "org_id": "org_abc",
 "data": {
  "score": 67,
  "band": "RED",
  "confidence": 88,
  "explanation": "Invariant relationships detected...",
  "evidence_pointer": "ev_9c8b7a"
 }
}
```


Security: HMAC-SHA256 signed payloads with X-Acd-Signature header **Delivery**: Exponential backoff retries up to 24h

C.6 Error Handling


```
{
 "error": {
```

```
  "type": "validation_error | auth_error | rate_limit | upstream_error | conflict | not_found | server_error",
  "code": "INVALID_FIELD | MISSING_SCOPE | ...",
  "message": "Human readable explanation",
  "details": [
   {"field": "price", "issue": "must be > 0"}
  ],
  "request_id": "req_01HF..."
 }
}
```

Appendix D – Operational Runbooks

D.1 Deployment Pipeline

Environments:

- **Dev**: Feature development, synthetic golden datasets
- **Staging**: Production mirror, anonymized client feeds
- **Production**: High-availability clusters, full compliance controls

CI/CD Process:

1. GitHub Actions triggered on merge → main branch
2. Docker images built for backend, frontend, analytics
3. Cosign signatures attached; hashes logged to transparency ledger
4. Helm chart deploys to staging Kubernetes cluster
5. Smoke tests run synthetic ICP/VMM checks against golden datasets
6. Human approval required before production promotion
7. Canary rollout (10% → 50% → 100%) with automated rollback triggers
8. Post-deploy checks: End-to-end contract tests, API health checks, latency benchmarks

Rollback Procedure:

- Canary monitors error rate >2% or latency >5s for >2 consecutive checks
- Automatic rollback triggered, alert escalated to SRE on-call
- Incident logged with deployment ID and git commit reference

D.2 Monitoring & Alerting

Monitoring Stack:

- **Metrics**: Prometheus → Grafana dashboards
- **Logs**: ELK stack (Elasticsearch, Logstash, Kibana)
- **Tracing**: OpenTelemetry → Jaeger

- **Security**: Falco + AWS GuardDuty

Key Metrics:

- Latency: p95 < 2s for risk queries
- Throughput: ≥50k datapoints/min ingestion
- Error Rate: <0.1% API errors
- ICP Convergence Rate: ≥95%
- VMM Convergence Rate: ≥90%
- SLA Uptime: ≥99.5% (baseline), 99.99% (Tier 3 clients)

Alert Classifications:

- **Critical**: API downtime >1m, failed risk score pipeline, unsealed secrets, DB unavailability
- **Warning**: Latency >4s p95, ICP/VMM convergence <80%, ingestion backlog >5m
- **Info**: CPU >70%, storage utilization >80%, approaching quota limits

Escalation Matrix:

- L1: Automated alert to on-call SRE via PagerDuty
- L2: Escalation to DevOps lead within 15m if unresolved
- L3: Executive + client notification within 1h for sustained outage

D.3 Incident Response

Incident Classification:

- **SEV-1 (Critical)**: Complete outage, client-facing data corruption
- **SEV-2 (High)**: Partial outage, SLA breach on latency/throughput
- **SEV-3 (Moderate)**: Functionality degraded, but business impact low
- **SEV-4 (Low)**: Cosmetic/UI issues, no client impact

Response Steps:

1. Detection: Alert via monitoring stack
2. Triage: L1 SRE validates scope/impact
3. Escalation: If SEV-1/2, L2 DevOps + incident commander engaged
4. Communication: Client notified within SLA window
5. Resolution: Apply hotfix, rollback, or failover
6. Postmortem: Root cause analysis (RCA) delivered to clients within 5 business days

D.4 Backup & Recovery

Backup Strategy:

- **Database**: Point-in-time recovery (PITR) with WAL shipping
- **Frequency**: Incremental every 15m, full backup every 24h

- **Retention**: 7 years (configurable per client contract)
- **Encryption**: AES-256 at rest, TLS 1.3 in transit

Recovery Objectives:

- **RPO (Recovery Point Objective)**: ≤15m
- **RTO (Recovery Time Objective)**: ≤1h

Testing:

- Quarterly backup restoration tests
- Randomized audit drills to validate RPO/RTO adherence
- Cryptographic proof of backup integrity (Merkle hash chain, anchored daily)

Appendix E – Evidence Bundle Specifications

E.1 Court-Ready Evidence Packages

Each evidence bundle contains:

- **Input manifest** (cryptographically hashed)
- **Environment configuration** and ICP/VMM parameters
- **Test statistics, p-values, confidence intervals**
- **Charts** (distribution plots, environment comparisons, network analysis)
- **Natural-language summary** generated by agent
- **Cryptographic signature** with RFC 3161 timestamping
- **Complete audit trail** with immutable log references

E.2 Supported Export Formats

PDF: Court filings and legal submissions

- Executive summary with risk classification
- Technical methodology appendix
- Statistical test results with confidence intervals
- Visual evidence (charts, distributions)
- Signed attestation of methodology compliance

JSON/XML: Regulatory ingestion systems

- Machine-readable test results
- Complete parameter configurations
- Audit trail references
- Digital signatures for verification

CSV: Internal audit and compliance review

- Raw statistical outputs
- Time-series risk evolution
- Environment sensitivity metrics
- Cross-validation results

E.3 Legal Admissibility Framework

Chain of Custody: Immutable cryptographic logs anchored daily **Methodological Transparency**: Published ICP/VMM derivations in appendices **Independent Validation**: Golden datasets allow replication of risk classifications **Format Compatibility**: Exports optimized for different judicial systems **Expert Testimony Support**: Qualified economists available for court proceedings

E.4 Optional External Anchoring

Default: Cryptographic hash-chained logs with RFC 3161 timestamping **Optional Enhancement**: Daily consolidated hash anchored to:

- Bitcoin timestamp authority
- Ethereum mainnet (enterprise contracts only)
- Independent third-party TSA services

Client Control: External anchoring disabled by default to reduce operational complexity; can be enabled for highest-stakes litigation through enterprise console

Appendix F – Compliance & Regulatory Framework

F.1 Basel III Alignment

Requirement	ACD Feature	Evidence/Implementation
Capital Adequacy (SRT)	Immutable audit trails of risk model outputs; timestamped and cryptographically signed	Audit logs + cryptographic anchoring (Merkle chain)
Model Risk Management	Dual-pillar econometric approach (ICP + VMM), transparent derivations	Appendix A (ICP) + Mathematical foundations
Operational Risk Controls	Automated monitoring + incident response runbooks	Appendix D (Runbooks)
Stress Testing	Synthetic golden datasets (competitive vs coordinated scenarios)	Backtesting framework

Disclosure Requirements	Agent-generated, court-ready evidence packages	Evidence bundle specifications

F.2 SOX (Sarbanes-Oxley) Alignment

Requirement	**ACD Feature**	**Evidence/Implementation**
Internal Controls over Financial Reporting	Immutable logs of all algorithmic monitoring cycles	RFC 3161 timestamping, verifiable with external auditors
Auditability	Verifiable risk classifications with provenance tracking	Audit trail APIs
Change Management	ITIL-aligned change control with deployment logs	Appendix D.1
Error Handling & Escalation	Tiered incident response with SEV-1–4	Appendix D.3
Annual Certification Support	Agent-generated compliance reports exportable in PDF/JSON	Compliance reporting module

F.3 GDPR & Data Protection

Principle	**ACD Implementation**
Lawfulness, Fairness, Transparency	Transparent econometric methodology; natural-language explanations of risk classifications
Data Minimization	Collects only necessary pricing/market data; anonymization applied to client feeds in staging
Accuracy	Continuous validation against golden datasets; explicit confidence intervals reported
Integrity & Confidentiality	AES-256 encryption at rest, TLS 1.3 in transit, fine-grained RBAC
Right to Access/Erasure	API endpoints for data export & purge; legal team integration for compliance requests
Cross-Border Data Transfers	Regional data residency options (EU-only clusters, US-only clusters)

F.4 Compliance Reporting

- **Quarterly Compliance Reports**: Delivered to clients for internal audit
- **On-Demand Reports**: Custom reports for regulatory inquiries
- **Audit Interfaces**: API endpoints allow auditors to query timestamped data directly
- **Regulatory Sandbox**: Pre-approval programs with competition authorities

Appendix G – Complete Compliance Matrix

G.1 GDPR & CCPA Detailed Alignment

Lawfulness, Fairness, Transparency:

- Transparent econometric methodology with published mathematical foundations
- Natural-language explanations of all risk classifications
- Clear data processing purposes documented in privacy notices
- Algorithmic decision-making transparency through agent explanations

Data Minimization:

- Collects only pricing/market data necessary for coordination detection
- Anonymization applied to all client feeds in staging environments
- Automatic data purging after retention periods
- Field-level encryption for any incidental PII

Accuracy:

- Continuous validation against golden datasets with documented accuracy metrics
- Explicit confidence intervals reported for all statistical outputs
- Data quality monitoring with automated correction procedures
- Cross-validation against independent market data sources

Integrity & Confidentiality:

- AES-256 encryption at rest with hardware-backed key management
- TLS 1.3 in transit with perfect forward secrecy
- Fine-grained RBAC with audit logging of all access
- Multi-tenant isolation with strict data boundaries

Right to Access/Erasure:

- Self-service API endpoints for data export in standard formats
- Automated deletion workflows with cryptographic proof of erasure
- Legal team integration for complex compliance requests
- Right to explanation for algorithmic risk classifications

Cross-Border Data Transfers:

- Regional data residency with client-selectable jurisdictions

- Standard Contractual Clauses (SCCs) for international transfers
- Data Processing Agreements (DPAs) with all sub-processors
- Adequacy decision compliance for EU-US transfers

G.2 Legal Admissibility Framework

Chain of Custody Requirements:

- Immutable cryptographic logs with RFC 3161 timestamping
- Complete provenance tracking from data ingestion to final outputs
- Tamper-evident storage with hash chain verification
- Independent timestamp authority validation

Methodological Transparency:

- Published ICP/VMM mathematical derivations in peer-reviewed format
- Open-source validation tools for independent verification
- Complete parameter disclosure with sensitivity analysis
- Expert witness availability for methodology explanation

Independent Validation:

- Golden datasets enable replication of all risk classifications
- Synthetic data generation for blind testing by third parties
- Cross-validation protocols with independent econometric tools
- Statistical significance testing with multiple correction methods

Format Compatibility:

- PDF exports optimized for court filing systems
- XML/JSON formats for regulatory database ingestion
- CSV outputs for forensic analysis tools
- Digital signature verification across all formats

Expert Testimony Support:

- Qualified economists available for deposition and trial testimony
- Pre-prepared testimony packages with visual aids
- Methodology training materials for legal teams
- Cross-examination preparation with common challenges addressed

G.3 Privacy by Design Implementation

Minimize: Only ingest fields necessary for stated coordination analysis **Pseudonymize**: Replace direct identifiers with tenant-scoped pseudonyms using cryptographic hashing **Purpose-binding**: Access policies strictly keyed to declared purposes (monitoring, litigation support, regulatory compliance) **Explainability**: All natural-language summaries include rationale and links to underlying statistical tests **Consent Management**: Granular consent

tracking with withdrawal mechanisms **Data Subject Rights**: Automated workflows for access, rectification, and erasure requests

G.4 Secure SDLC & Supply Chain

Development Security:

- Threat modeling for every feature touching classified data
- Security gates in CI/CD with automated SAST/DAST scanning
- Dependency scanning with vulnerability database integration
- Infrastructure-as-Code (IaC) security validation
- Software Bill of Materials (SBOM) published per release

Code Review Process:

- Mandatory security review for all changes touching C3/C4 data classification
- Two-person approval required for production deployments
- Automated policy compliance checking in pull requests
- Security architecture review for significant feature additions

Supply Chain Security:

- Pinned dependency versions with hash verification
- Container image signing with cosign/sigstore
- Admission controller blocking unsigned images in production
- Regular security updates with automated testing pipelines

Penetration Testing:

- Annual third-party security assessments with remediation tracking
- Client-sponsored testing programs welcome with coordinated disclosure
- Bug bounty program for responsible vulnerability disclosure
- Remediation SLAs: Critical (24h), High (72h), Medium (30d)

G.5 Vendor & Third-Party Risk Management

Due Diligence Process:

- Data Protection Impact Assessments (DPIAs) for all processors
- SOC 2 Type II / ISO 27001 attestations required
- Financial stability assessment for critical vendors
- Data Processing Agreements (DPAs) with termination and return clauses

Key Third Parties:

- Cloud infrastructure providers (AWS/GCP) with BAAs and DPAs
- Managed database services with encryption at rest guarantees
- Email/SMS alerting services with data residency controls

- Optional timestamp authorities with independent audit trails

Continuous Assessment:

- Quarterly vendor scorecards with security posture tracking
- Automated alerts on security certification expirations
- Supply chain monitoring for security incidents
- Annual vendor risk assessment reviews with executive approval

G.6 Customer Controls & Admin Console

Organizational Policies:

- Configurable MFA requirements (TOTP, WebAuthn, SMS)
- Session timeout controls (15m - 8h configurable)
- IP allow-listing with CIDR block support
- Data export approval workflows with dual control

Key Management:

- Customer-managed keys (CMK) support for C4 data classification
- Bring Your Own Key (BYOK) integration with major KMS providers
- Key rotation policies with automated compliance reporting
- Hardware Security Module (HSM) integration for high-security requirements

Audit Access:

- Self-serve access to immutable logs through web console
- API endpoints for programmatic audit log retrieval
- Evidence manifests exportable for regulatory submissions
- Real-time compliance dashboard with SLA tracking

Data Governance:

- Data classification tagging with automated policy enforcement
- Retention policy management with legal hold capabilities
- Cross-border transfer controls with jurisdiction validation
- Data lineage tracking with impact analysis tools

Appendix H – Complete API Specifications

H.1 Authentication Architecture

OAuth2 Implementation:

Token Endpoint: POST https://auth.acd-monitor.com/oauth/token
Grant Types: client_credentials, authorization_code

Scopes: read:analytics, write:analytics, read:evidence, write:evidence, read:events, write:events, read:audit, admin:org
Token Lifetime: Access (15m), Refresh (24h)
Signature: RS256 with rotating keys

Multi-Factor Authentication:

- TOTP (RFC 6238) with 30-second windows
- WebAuthn/FIDO2 for hardware token support
- SMS backup with rate limiting (max 3/hour)
- Recovery codes (10 single-use codes per user)

Service-to-Service Authentication:

- Mutual TLS (mTLS) for high-trust integrations
- Workload identity federation (GCP/AWS IAM)
- API key authentication for legacy systems
- JWT bearer tokens with custom claims

H.2 Complete Endpoint Catalog

Agent Intelligence Endpoints:

POST /api/v1/agent/chat - Interactive agent conversations
GET /api/v1/agent/conversations - List conversation history
DELETE /api/v1/agent/conversations/{id} - Delete conversation
POST /api/v1/agent/explain - Explain specific risk findings
POST /api/v1/agent/summarize - Generate executive summaries

Risk Assessment Endpoints:

GET /api/v1/risk/summary - Current risk overview
GET /api/v1/risk/history - Historical risk evolution
GET /api/v1/risk/forecast - Predictive risk modeling
GET /api/v1/risk/alerts - Active risk alerts
POST /api/v1/risk/thresholds - Configure alert thresholds

Analytics Endpoints:

GET /api/v1/analytics/icp-results - Invariant Causal Prediction outputs
GET /api/v1/analytics/vmm-results - Variational Method of Moments outputs
GET /api/v1/analytics/coordination-index - Current coordination metrics
GET /api/v1/analytics/environment-sensitivity - Market adaptation analysis
POST /api/v1/analytics/custom-tests - Run custom statistical tests

Data Management Endpoints:

POST /api/v1/data/ingest/prices - Upload pricing data
POST /api/v1/data/ingest/events - Upload market events
POST /api/v1/data/ingest/batch - Bulk data upload
GET /api/v1/data/sources/status - Data source health check
GET /api/v1/data/quality/metrics - Data quality dashboard
POST /api/v1/data/validation/rules - Configure validation rules

Evidence & Reporting Endpoints:

POST /api/v1/evidence/generate - Create evidence bundles
GET /api/v1/evidence/bundles/{id} - Retrieve evidence bundle
GET /api/v1/evidence/bundles - List evidence bundles
POST /api/v1/reports/compliance - Generate compliance reports
POST /api/v1/reports/executive - Generate executive summaries
GET /api/v1/reports/templates - Available report templates

Audit & Compliance Endpoints:

GET /api/v1/audit/logs - Query audit trail
GET /api/v1/audit/events - System event history
GET /api/v1/compliance/status - Compliance dashboard
GET /api/v1/compliance/policies - Active compliance policies
POST /api/v1/compliance/export - Export compliance data

Administration Endpoints:

POST /api/v1/admin/users - User management
GET /api/v1/admin/organizations - Organization settings
PUT /api/v1/admin/quotas - Update usage quotas
GET /api/v1/admin/billing - Billing and usage metrics
POST /api/v1/admin/tokens - API token management

H.3 Request/Response Schemas

Risk Summary Schema:

```
{
  "score": "integer [0,100]",
  "band": "LOW | AMBER | RED",
  "confidence": "integer [0,100]",
  "lastUpdated": "RFC3339 timestamp",
```

```
  "source": {
    "freshnessSec": "integer >=0",
    "dataFeeds": ["string"],
    "quality": "float [0,1]"
  },
  "explanation": "string",
  "coordinationIndex": "float",
  "environmentSensitivity": "float",
  "statisticalSignificance": "float [0,1]"
}
```

Evidence Bundle Schema:

```
{
  "bundle_id": "string",
  "status": "PENDING | PROCESSING | READY | FAILED",
  "created_at": "RFC3339",
  "completed_at": "RFC3339 | null",
  "file_name": "string",
  "size_bytes": "integer",
  "download_url": "string",
  "expires_at": "RFC3339",
  "contents": {
    "risk_summary": "boolean",
    "metrics": "boolean",
    "events": "boolean",
    "chat_context": "boolean",
    "statistical_tests": "boolean",
    "audit_trail": "boolean"
  },
  "digital_signature": "string",
  "hash_chain": "string"
}
```

H.4 WebSocket Real-Time API

Connection Endpoint: wss://api.acd-monitor.com/v1/stream

Authentication: Bearer token in Authorization header or ?token= query parameter

Subscription Management:

```
// Subscribe to risk updates
{
  "action": "subscribe",
```

```
  "channel": "risk.updates",
  "filters": {
    "productIds": ["cds-fnb-5y"],
    "riskThreshold": "AMBER"
  }
}

// Subscribe to system events
{
  "action": "subscribe",
  "channel": "system.events",
  "filters": {
    "severity": ["HIGH", "CRITICAL"]
  }
}
```

Event Formats:

```
// Risk update event
{
  "type": "risk.update",
  "timestamp": "2025-09-11T20:40:00Z",
  "productId": "cds-fnb-5y",
  "riskScore": 68,
  "classification": "AMBER",
  "delta": +15,
  "explanation": "Increased cross-price sensitivity detected"
}

// System event
{
  "type": "system.alert",
  "timestamp": "2025-09-11T20:41:00Z",
  "severity": "HIGH",
  "component": "vmm.convergence",
  "message": "VMM convergence failure rate exceeding threshold"
}
```

H.5 Rate Limiting Implementation

Tier-Based Limits:

```
Silver Tier:
- API Requests: 10,000/min (burst 20,000)
```

- Data Ingestion: 50MB/min
- Evidence Generation: 5 concurrent bundles
- WebSocket Connections: 10 concurrent

Gold Tier:
- API Requests: 20,000/min (burst 40,000)
- Data Ingestion: 200MB/min
- Evidence Generation: 20 concurrent bundles
- WebSocket Connections: 50 concurrent

Platinum Tier:
- API Requests: 50,000/min (burst 100,000)
- Data Ingestion: 1GB/min
- Evidence Generation: 100 concurrent bundles
- WebSocket Connections: 200 concurrent

Rate Limit Headers:

X-RateLimit-Limit: 10000
X-RateLimit-Remaining: 9500
X-RateLimit-Reset: 1641024000
X-RateLimit-Tier: silver

H.6 Error Handling & Status Codes

Standard HTTP Status Codes:

- 200 OK - Successful request
- 201 Created - Resource created successfully
- 202 Accepted - Request accepted for processing
- 400 Bad Request - Invalid request format/parameters
- 401 Unauthorized - Authentication required
- 403 Forbidden - Insufficient permissions
- 404 Not Found - Resource not found
- 409 Conflict - Resource conflict
- 422 Unprocessable Entity - Validation errors
- 429 Too Many Requests - Rate limit exceeded
- 500 Internal Server Error - Unexpected server error
- 502 Bad Gateway - Upstream service error
- 503 Service Unavailable - Service temporarily unavailable

Error Response Format:

```
{
  "error": {
```

```
  "type": "validation_error",
  "code": "INVALID_FIELD_VALUE",
  "message": "Field 'price' must be a positive number",
  "details": [
   {
    "field": "price",
    "value": -10.5,
    "constraint": "must be > 0"
   }
  ],
  "request_id": "req_01HF8X2K9R7ZQ4M6P3J5N8B0",
  "timestamp": "2025-09-11T20:45:00Z",
  "documentation": "https://docs.acd-monitor.com/errors#INVALID_FIELD_VALUE"
 }
}
```


H.7 Pagination & Filtering

Cursor-Based Pagination:

GET /api/v1/audit/logs?cursor=eyJpZCI6IjEyMyJ9&limit=50

Response:


```
{
 "items": [...],
 "pagination": {
  "next_cursor": "eyJpZCI6IjE3MyJ9",
  "has_more": true,
  "total_count": 1250
 }
}
```


Advanced Filtering:

GET /api/v1/risk/history?timeframe=30d&productId=cds-fnb-5y&riskBand=RED,AMBER&sort=timestamp:desc

Query Parameters:
- timeframe: 1h, 24h, 7d, 30d, 3m, 6m, 1y, ytd, custom
- productId: Filter by specific product identifiers
- riskBand: LOW, AMBER, RED (comma-separated)
- sort: field:direction (asc/desc)
- limit: 1-1000 (default 50)

- cursor: Pagination cursor

H.8 Webhook Configuration & Delivery

Webhook Management:

```
POST /api/v1/webhooks
{
 "url": "https://client.example.com/acd-webhooks",
 "events": ["risk.alert", "evidence.ready"],
 "secret": "whsec_...",
 "enabled": true,
 "retry_policy": {
  "max_attempts": 5,
  "backoff_multiplier": 2,
  "max_backoff": "1h"
 }
}
```

Webhook Security:

- HMAC-SHA256 signature in X-ACD-Signature header
- Timestamp verification with 5-minute tolerance
- Replay protection via X-ACD-Event-Id header
- SSL/TLS certificate validation required

Delivery Guarantees:

- At-least-once delivery with deduplication support
- Exponential backoff retry (1s, 2s, 4s, 8s, 16s)
- Dead letter queue after max retry attempts
- Webhook health monitoring with automatic disabling

Document Version: 2.2
Last Updated: January 2025
Next Review: March 2025
Classification: Public Product Specification

Page Count: Complete enterprise-grade specification covering all technical, operational, compliance, and commercial requirements for algorithmic coordination detection and monitoring platform.

Author: Ygor Francisco