FinSeminarIQ™

Technical Architecture Abstract

Turn Retirement Dinner Attendees Into Clients

Prepared by Axon Tech Labs

axontechlabs.com

2026

FinSeminarIQ™ - Technical Architecture Abstract

Axon Tech Labs | axontechlabs.com | 2026

Overview

FinSeminarIQ is a fully serverless, event-driven platform built exclusively on AWS managed services. There are no servers to manage, no containers to orchestrate, and no idle compute costs. Every component scales automatically and bills only for actual usage.

Each client deployment is a completely isolated AWS account — no shared infrastructure, no shared data plane, no multi-tenancy at the application layer.

AWS Service Stack

The platform is built exclusively on AWS managed services across seven layers:

Layer	Service	Purpose
Compute	AWS Lambda (Python 3.13)	All application logic
API	Amazom API Gateway	Request routing, JWT auth, rate limiting
Primary data store	Amazon DynamoDB	Source of truth for all transactional data
Analytics warehouse	Amazom Redshift Serverless	Star schema analytics and reporting
Object storage	Amazon S3	QR codes, PDFs, pool uploads, mail house exports
Secrets	AWS Secrets Manager	JWT signing keys, admin credentials
DNS + TLS	Amazon Route 53 + AWS ACM	Custom domain, auto-renewing TLS certificates
Observability	Amazom CloudWatch	Lambda logs, metrics, billing alarms
BI + AI	Amazon QuickSight + Amazon Q	Nine dashboards, SPICE engine, generative AI

Authentication Architecture

Admin Application

Amazon Cognito user pools with per-office role isolation. Office admins see only their own data. Superuser role spans all offices. JWT tokens are RS256-signed using RSA-2048 keys stored in Secrets Manager — never in environment variables or Lambda configuration.

Registration and Questionnaire Forms

Stateless JWT tokens embedded in QR codes. Each QR encodes a signed token containing the campaign ID, prospect ID, and expiry. The Lambda verifier validates the signature against the public key in Secrets Manager. No session state, no cookies, no database lookup required to authenticate a form submission.

Data Pipeline

Lambda connects to Redshift Serverless using IAM authentication — no Redshift password exists anywhere in the system. The Lambda execution role is granted database access via SQL GRANT statements — the IAM role is the credential. No passwords stored, no rotation required.

Data Model

DynamoDB uses a single-table design with composite keys. All records for a client live in one table partitioned by entity type:

Partition Key	Sort Key
COMPANY#{company_id}	METADATA
COMPANY#{company_id}	SUPPRESSION#{identity_hash}
COMPANY#{company_id}	PUSH_LOG#{ulid}
OFFICE#{office_id}	METADATA
OFFICE#{office_id}	VENUE#{venue_id}
OFFICE#{office_id}	POOL#{pool_id}
OFFICE#{office_id}	POOLPROSPECT#{pool_id}#{prospect_id}
OFFICE#{office_id}	MAILARCHIVE#{mailed_at_date}#{identity_hash}
CAMPAIGN#{campaign_id}	METADATA
CAMPAIGN#{campaign_id}	PROSPECT#{prospect_id}
CAMPAIGN#{campaign_id}	RSVP#{prospect_id}
CAMPAIGN#{campaign_id}	WAITLIST#{prospect_id}
CAMPAIGN#{campaign_id}	ANSWERS#{prospect_id}
EVENT#{event_id}	METADATA
MAILHOUSE_JOB#{campaign_id}	STATUS
MAPPINGPROFILE#{profile_id}	METADATA
CONFIG#GLOBAL	KEY#{parameter_name}

Cross-campaign suppression is enforced at the COMPANY# partition level — a prospect's identity hash is a deterministic hash of name and address, written once when they attend any event and checked against all future campaign materializations across all offices.

Analytics Pipeline

Transactional data flows from DynamoDB into Redshift Serverless via an AWS Step Functions state machine — no timeout ceiling, no manual intervention required.

Pipeline Stages

- Extract — Lambda scans DynamoDB and writes staging files to S3
- Transform — Lambda maps DynamoDB items to Redshift row format
- Load — Lambda executes bulk DELETE and batched INSERT into Redshift

Redshift Schema

- Fact tables: events, prospects, answers, registrations, companies, offices
- Scoring views: composite wealth index percentile ranked within each campaign pool
- Segmentation views: seven deterministic planning clusters assigned from questionnaire responses
- Funnel views: prospect journey from materialized through attended, submitted, and consultation requested
- Dashboard views: denormalized, QuickSight-ready views powering all nine dashboards

Performance

Ingest strategy uses bulk DELETE followed by batched single-VALUES INSERT per table, wrapped in a single transaction. On any failure the transaction rolls back automatically — tables are left in their pre-ingest state, safe to re-invoke without manual cleanup.

Redshift enforces a 32,767 bind parameter limit per prepared statement. Ingest batches are sized per table to stay under this limit. Full pipeline completes in seconds on a warm instance — subsequent pushes are minimal since pools and completed campaigns are synced only once. First run after an idle period may take longer while Redshift Serverless wakes up.

Prospect Wealth Scoring

Every prospect is scored at campaign materialization time using a five-component composite index. Scoring uses percentile ranking within the filtered campaign pool — not absolute dollar thresholds. A score of 85 means this prospect ranks above 85% of candidates in this specific campaign's geography.

Component	Weight
Net worth	35%
Investable assets	25%
Household income	20%
Home value	10%
Discretionary income rating	10%

The score resets per campaign and automatically adapts to local market conditions — a high score in a dense coastal market and a high score in a rural inland market both mean the same thing: top of the local field.

Prospect Tiers

Tier	Score
VIP Private Wealth Targets	Score >= 75
Core Growth Opportunities	Score 50-74
Nurture & Mass Market	Score < 50

Network and Security Architecture

All Lambda functions run inside a client VPC in private subnets with no direct internet access. All traffic to AWS services routes through VPC gateway and interface endpoints — no NAT gateway, no public internet traversal.

Security Group Rules

- Lambda → Redshift on port 5439 only
- Lambda → DynamoDB via gateway VPC endpoint — no NAT traversal
- Lambda → Secrets Manager via interface VPC endpoint
- No 0.0.0.0/0 rules anywhere in the data plane
- Lambda → S3 via gateway VPC endpoint — no NAT traversal

Public-Facing Endpoints

All public-facing endpoints — the registration form and questionnaire form — are served through Amazon API Gateway with JWT validation enforced at the Lambda layer. The admin application is behind Amazon Cognito — unauthenticated requests never reach the Lambda functions.

Encryption

Layer	Standard
Data in transit	TLS 1.3 enforced on all endpoints
Data at rest	AES-256 on DynamoDB, Redshift, and S3
Key management	AWS KMS- client KMS key supported

Operator Access Model

Axon Tech Labs maintains the platform using a cross-account IAM role created in the client's account during onboarding. This role is explicitly scoped.

Permitted Actions

- CloudFormation stack updates
- Lambda code deployments
- CloudWatch Logs read access
- SSM Parameter Store under /finadvisor/* path only
- CDK bootstrap resources

Explicitly Denied

- DynamoDB data plane — GetItem, Scan, Query, PutItem
- Redshift data plane
- S3 paths containing prospect data or generated files
- Secrets Manager GetSecretValue

Axon Tech Labs cannot read prospect records, questionnaire answers, or authentication credentials. This is enforced by IAM policy, not by convention.

Every API call made under the operator role is logged in the client's AWS CloudTrail. The client can audit the full history of Axon Tech Labs activity at any time. Access can be revoked instantly by the client without legal process.

Deployment Model

Each client deployment is parameterized via AWS CDK context — no code changes between clients, only configuration values. Six CDK stacks deploy in sequence:

- NetworkStack — VPC, subnets, NAT gateway, security groups, VPC endpoints
- StorageStack — DynamoDB table, S3 bucket, GSI configuration
- ParameterStack — SSM Parameter Store entries for all configuration values
- LambdaStack — all Lambda functions, execution roles, environment configuration
- ApiStack — API Gateway, Cognito authorizer, route definitions
- FrontendStack — Route 53 DNS, ACM certificate

Target onboarding time from operator role creation to first admin login: under one business day.

New office onboarding after initial deployment requires no infrastructure changes — offices are DynamoDB records. Adding an office is a data operation, not a deployment.

Compliance Posture

The platform is designed for FINRA/SEC-regulated environments where data residency and vendor access controls are compliance requirements, not preferences.

Requirement	Implementation
Data residency	All data in client's AWS account, client chosen region
Encryption at rest	AES-256 on DynamoDB, Redshift, and S3. Client KMS key supported
Encryption in transit	TLS 1.3 enforced on all endpoints
Access control audit	Full CloudTrail logging of all Axon Tech Labs operator actions
Vendor data access	Explicitly blocked by IAM policy – not by convention
Data portability	Client can export all data at any time
Contract termination	Client deletes operator IAM role – access revoked immediately
Multi-client isolation	Separate AWS account per client – no shared infrastructure

Current Limitations

The following items are outside the scope of the current version and are noted here for transparency.

CRM Integration

The platform does not currently have a native sync to Salesforce, Wealthbox, or Redtail. Prospect and questionnaire data is exportable from the admin application and from Redshift. A webhook or API integration layer is on the roadmap.

SSO and SAML Federation

Authentication is handled by Amazon Cognito. SAML 2.0 federation with an enterprise identity provider is supported by Cognito but not configured in the current deployment. This is an onboarding option, not a product gap.

SOC 2 Certification

The platform runs on AWS infrastructure that holds SOC 2 Type II certification. The application layer itself has not undergone a separate SOC 2 audit. Clients operating under strict vendor compliance requirements should note this distinction.