Asora — Security & Architecture Overview

Platform Overview

Asora is a cloud-native wealth management platform purpose-built for family offices, wealth advisers, and their clients. The platform is delivered as a fully managed SaaS solution hosted on Microsoft Azure, providing secure access to portfolio data, reporting, document management, and client communications.

Data Isolation & Tenant Separation

Every client organisation operates within a dedicated, isolated database. There is no shared data store between tenants — each client's financial data, documents, and configuration reside in their own Azure SQL Database instance. This architecture ensures:

- Complete logical separation
- Independent lifecycle management — backups, retention, and data residency are managed per tenant
- Reduced blast radius — a misconfiguration or incident affecting one tenant cannot impact another

Tenant identity is verified on every API request through secure token claims, ensuring requests are always routed to the correct isolated environment.

Encryption

In transit: All data in motion is encrypted using TLS 1.2+ across every connection — between client browsers and the platform, between internal services, and between the platform and Azure SQL databases.

At rest: All data stored in Azure SQL Database and Azure Blob Storage is encrypted at rest using AES-256 encryption managed by Microsoft Azure. In addition, Asora applies field-level encryption to sensitive data elements within the database, providing an extra layer of protection beyond standard storage encryption.

Secrets management: All application secrets, API keys, and certificates are stored in Azure Key Vault — never in application code or configuration files. Access to Key Vault is governed by Azure Workload Identity, ensuring only authorised services can retrieve secrets at runtime.

Cloud Infrastructure & Deployment

Asora is deployed on Azure Kubernetes Service (AKS), providing:

- High availability — workloads are distributed across multiple nodes with automatic failover
- Auto-scaling — infrastructure scales dynamically to meet demand
- Geo-redundant deployment — primary region West Europe with secondary region North Europe, supporting resilience and EU data residency requirements
- Immutable deployments — every release is deployed as a versioned container image, ensuring consistency and rollback capability
- Network security — traffic enters through Azure Application Gateway with Web Application Firewall (WAF) capabilities and TLS termination; internal service-to-service communication is contained within the cluster network

All container images are stored in a private Azure Container Registry, scanned and accessible only to the Asora deployment pipeline.

Backups & recovery: Automated database backups are maintained with regularly tested restore procedures, ensuring data can be recovered in line with business continuity requirements.

Authentication & Access Control

User authentication is handled through an OAuth 2.0/OpenID Connect identity provider with support for multi-factor authentication (MFA). Access tokens are short-lived and scoped to specific APIs, ensuring users & services operate with least-privilege access.

Role-based access control is enforced at every API endpoint with support for Admin, Standard, and Adviser roles. All controllers require authentication by default — public endpoints are explicitly opt-in, never the default.

Granular permissions allow access to be controlled at the organisation, family group, portfolio, account, and document level ensuring users see only what they are authorised to access.

Application Security

- Content Security Policy (CSP) headers restrict which resources browsers can load, mitigating cross-site scripting risks
- CORS policies are strictly whitelisted to Asora domains only

- Security headers including `X-Content-Type-Options`, `X-Frame-Options`, and `Referrer-Policy` are applied to all responses
- Input validation is enforced on both client and server side
- No direct database exposure — all data access flows through authenticated API endpoints with parameterised queries, eliminating SQL injection risk

Monitoring & Incident Response

The platform is monitored using Azure Application Insights for real-time telemetry, performance tracking, and anomaly detection. Structured logging captures operational events without recording personally identifiable information (PII).

A documented incident management process is in place with defined severity levels, escalation paths, and customer communication procedures.

Software Development Lifecycle

- Controlled release process — all changes progress through Dev, QA, UAT, and Production with strict promotion controls
- Automated testing — unit, UI, and performance testing enforced as release quality gates
- Security scanning — automated vulnerability and code quality scanning applied early in the pipeline
- Mandatory peer review — all releases follow a structured review process with documented risk assessment and traceability

Compliance & Certifications

Asora operates under an ISO 27001 certified Information Security Management System (ISMS), demonstrating a structured and audited approach to:

- Risk assessment and treatment
- Access control and identity management
- Incident management and business continuity
- Secure software development practices
- Supplier and third-party risk management

Asora is hosted on Microsoft Azure, which itself maintains ISO 27001, SOC 1/2/3, and numerous other certifications. Asora inherits and builds upon Azure's compliance posture.

GDPR alignment: All client data is stored and processed within EU regions, and operational controls are designed to support GDPR compliance requirements.