Access and Setup Requirements Documentation

Client Information

Field	Value
Client Name	Vantage Financial
Report Type	Access and Setup Requirements Analysis
Generated By	ASRD Definer System
Report Date	2025-12-03 12:20:00

Executive Summary

This report presents comprehensive documentation of access and setup requirements needed between Subatomic and the Client to enable the TO-BE data flows, AI solutions, and processes. It includes system access requirements, integration setup, cloud infrastructure needs, AI solution access requirements, data access requirements, and gap analysis.

Report Overview

Section	Description	Status
Access and Setup Requirements Analysis	Comprehensive requirements analysis	✓ Completed

---

Access and Setup Requirements Analysis

Overview

This section provides comprehensive documentation of all access and setup requirements needed between Subatomic and the Client to enable the TO-BE architecture. It includes system access modeling, integration and credential setup, cloud infrastructure requirements, AI solution access requirements, data access requirements, actor setup responsibilities, and gap analysis.

Requirements Summary

Component	Description	Status
System Access Requirements	Access provisioning for all systems	Documented
Integration Setup	System-to-system connection configuration	Documented
Cloud Infrastructure	Cloud resources and infrastructure needs	Documented
AI Solution Access	Access requirements for AI Agents and Workflows	Documented
Data Access Requirements	Data source access configuration	Documented
Gap Analysis	Identified gaps and proposed solutions	Documented

Access and Setup Requirements Analysis

Executive Summary

This document synthesizes all setup, credentialing, and access requirements for enabling the TO-BE data architecture and Subatomic AI Agent platform at Vantage Financial. It details provisioning for all critical systems and cloud resources, secure connectivity (API/service accounts), actor responsibilities, and required configurations to automate client meeting prep, data aggregation, and compliance according to business and technical objectives. Key dependencies include full system API integrations (Redtail, Black Diamond, RightCapital, Wealthscape, Schwab, etc.), secure hybrid cloud/on-prem deployment, and permissioned access for both human users and modular AI agents. Several integration and access gaps remain, requiring collaborative resolution across IT/security (FinGuard), system vendors, and ops/back-office teams.

System Access Requirements

Table: System Access Matrix

System / Tool	Purpose	Access Required (Role/Persona)	Access Level & Type	Provisioning Method	Status
Subatomic Platform	AI Cognitive Workflows/Co-Worker Agents	AI solution admin/Ops, FinGuard IT, Vendor	Admin, config, service acct	Manual user/admin assign	Pending
Redtail CRM	Client data, meetings, tasks, workflows	AI agents, Paraplanners, Advisors, Ops	Read/write via API for AI, R/W UI for staff	OAuth2 SSO, API keys, user creds	In-progress (API/AIs), active (staff)
RightCapital	Financial planning, projections, data sync	AI agents, Paraplanners, Advisors	Read/write via API for AI; UI for staff	API keys/service acct, user creds	Pending (AI/API), active (staff)

System / Tool	Purpose	Access Required (Role/Persona)	Access Level & Type	Provisioning Method	Status
Black Diamond	Portfolio/performance reporting	AI agents, Paraplanners, Advisors	Read via API, export for AI; UI for staff	API/service acct, user creds	In progress (API setup), active (staff)
Wealthscape/Fidelity	Custodian data/ transactions	AI agents, Paraplanning, Ops, FinGuard (admin)	Read via API/file for AI; R/W UI for staff	Secure API key/service acct, SSO, possible manual file ingest	Pending (API for AI), active (manual)
Schwab	Custodian data/ transactions	AI agents, Ops, Paraplanning	Read via API/file (AI), R/W UI (staff)	API key/service acct, manual file, user creds	Pending (API), active (manual)
Shared Drives (Teams/SharePoint)	Output/document storage	AI agents, Advisors, Paraplanners, Ops	Read/write via API (AI), UI (staff)	Azure AD/SSO, API app registration	In progress
Microsoft Teams/ Email/Slack/Portal	Workflow triggers/ delivery	AI agents, Advisors, Ops, Paraplanning	Read/write channels (AI), messaging	OAuth2 SSO, app registration, webhook	In progress/Partial
Data Warehouse	Structured, transactional data store	AI agents, Ops, Analytics, Compliance	Read/write service acct (AI), R/W Admin	Cloud IAM (service account), manual add	To be created
Vector Store	Unstructured document/semantic search	AI agents, Ops, Compliance, Analytics	Read/write service acct (AI), admin	Cloud IAM/service acct, admin config	To be created
RetireUp	Scenario planning/data	AI agents, Paraplanners, Advisors	API read, UI (staff)	API keys/service acct, user creds	Pending
Riskalyze/Nitrogen	Risk analytics	AI agents, Paraplanner, Advisors	API read, UI (staff)	API key/service acct	Pending
Fathom	Analytics/reporting	AI agents, Advisors, Ops	API read, UI (staff)	API key/service acct	Pending

Key Notes:
- All production access for AI agents must be scoped, non-human service accounts with least privilege.
- Human-in-the-loop users (advisors, paraplanning, ops, etc.) retain interactive access via SSO or user-specific credentials.
- Vendor and FinGuard need admin-level access for platform maintenance and security.

Integration and Credential Setup

Table: System Integrations & Credentials

Source	Destination	Connection Method	Authentication	Credential Type	Setup Status	Dependencies
Redtail CRM	Subatomic Platform	REST API/Webhook	OAuth2/API Key	Service account	Pending	Redtail API, admin
RightCapital	Subatomic Platform	REST API	API Key/OAuth2	Service account	Pending	Vendor enablement
Black Diamond	Subatomic Platform	REST API/Data Export	API Key/OAuth2, token	Service account	In progress	Vendor coordination
Wealthscape	Subatomic Platform	REST API/File Transfer	Secure API, SSO	Service account	Pending	Custodian/FinGuard
Schwab	Subatomic Platform	REST API/File Transfer	API Key/Manual	Service account, file watcher	Pending	Vendor access
RetireUp	Subatomic Platform	REST API/Webhook	API Key	Service account	Pending	Confirm API
Riskalyze/Nitrogen	Subatomic Platform	REST API	API Key/OAuth2	Service account	Pending	Confirm API
Shared Drives	Subatomic Platform	File API/App Registration	OAuth2, app reg	App reg/service acct	In progress	Azure AD/IT involvement
Data Warehouse	Subatomic Platform	JDBC/ODBC/Cloud API	Service account/Key	Cloud IAM	Not started	Infrastructure ready
Vector Store	Subatomic Platform	API/SDK	Service account	Cloud IAM	Not started	Setup vector infra
Subatomic Output Agent	Teams/Email/ Slack	API/Webhook	OAuth2/App reg	App reg/service acct	In progress	IT approval, vendor

Credential/Token Management Considerations:
- Centralized credential vault (e.g., Azure Key Vault, AWS Secrets Manager) for all production integration secrets.
- Rotating API keys/service accounts at defined intervals.
- Audit logging and least privilege enforced on all integration accounts.

Transformation/Prep Needs:
- All inbound data traverses staging/ETL layer; schemas mapped, IDs deduplicated, compliance overlays applied.
- Configuring connectors may require custom scripts/adaptors for platforms lacking modern APIs.

Cloud Infrastructure Requirements

Cloud Architecture Overview

- **Cloud Provider:** Azure (preferred for Microsoft ecosystem fit); alternatives possible per final IT/Security sign-off
- **Core Infrastructure Components:**
  - Virtual Network, Subnets (for agent platform isolation)
  - Managed database/service for Data Warehouse (e.g., Azure SQL, Synapse)
  - Managed vector database (e.g., Azure Cognitive Search, Pinecone/other compliant with on-prem rules)
  - Blob Storage/S3-equivalent for ETL staging and intermediate files
  - Compute for workflow orchestration (App Services, Containers, or VM cluster)
  - Key Vault/Secrets Manager for credential storage
  - RBAC/IAM for resource access control
- **Access Requirements:**
  - Only subnet/hosted within Vantage IT perimeter (per infosec/compliance)
  - Service accounts for all AI agents and pipelines (scoped per resource)
  - Audit trails for all access and deployment actions
- **Service Accounts/IAM Roles:**
  - AI agents: read/write roles to databases, storage, log pipeline output
  - FinGuard/IT admin: global admin, resource provision, monitoring, access reviews
  - Ops/back office: limited observer roles for auditing and troubleshooting
- **Setup Dependencies:**
  - Resource group/project provisioning before connector/API registration
  - Security/tenant config by IT/FinGuard before data upload
  - All cloud services configured for data encryption (at rest/in transit)
  - Firewall and network rules to restrict ingress/egress per firm controls

AI Solution Access Requirements

AI Co-Worker Agents & AI Cognitive Workflow Platform

- **Which AI Solutions Need Access?**
  - All Subatomic AI Co-Worker Agents (Data Collection, Analyst, Advisor, Output, Distribution, Compliance Agent [future])
  - Cognitive Workflow Orchestrator/Core platform
- **Systems/Data Sources to Access:**
  - All production data integrations (Redtail, RightCapital, Black Diamond, Wealthscape, Schwab, risk/planning platforms, Fathom, [RetireUp])
  - All storage/analytics platforms (Data Warehouse, Vector Store, Shared Drives)
  - Communication channels as output (Teams, Email, Slack, Portal)
- **Authentication Methods:**
  - Service accounts/API keys (unique per system or integration, not shared with human users)
  - OAuth2 with app registration (preferred for MS ecosystem, Teams/SharePoint/Outlook/Slack)
  - Secure credential retrieval via Key Vault/Secrets Manager (never hard-coded)
- **Special Permissions:**
  - Read/write access to production data stores (scoped by function and system)
  - Permission to send messages/upload files in all designated output channels
  - Permission to trigger workflows/notifications in Teams, Slack, Email (with audit logged)
  - For future compliance agent, read access to all audit logs and compliance overlays
  - Only access data required for each role ("least privilege" model per agent persona)
- **Actor/Workflow Access:**
  - Human users (advisors/paraplanners/ops) initiate/review via UI; authentication via SSO or email login tied to cloud identity

Data Access Requirements

Table: Data Access Matrix

Data Source	Data Type	Access Method	Auth Requirements	Data Transformation/Prep	Compliance/ Restriction
Redtail CRM	Client, meeting, workflow	REST API	OAuth2/API key	Normalize client/object IDs	Data privacy, audit
RightCapital	Projections, scenarios	REST API	API Key/service acct	Map to standardized account model	PII, compliance logs
Black Diamond	Portfolio, reports	REST API/ export	API Key/service acct	Extract, clean, deduplicate	PII, role restrictions
Wealthscape/ Fidelity	Custodian, transactions	REST API, file	API/service acct	ETL from file/API, reconcile IDs	SOX, Reg BI, data vault
Schwab	Custodian, transactions	REST API, file	API/service acct	ETL, deduplicate accounts	SOX, data vault
RetireUp	Scenario, unstructured	API/manual	API key	Document extraction, embed	N/A
Riskalyze/Nitrogen	Risk, scoring	API/manual	API key	Structure for inputs/outputs	N/A

Data Source	Data Type	Access Method	Auth Requirements	Data Transformation/Prep	Compliance/ Restriction
Shared Drives	Document storage	File API	OAuth2/app reg	Version/rename, tag compliance	Data retention policy
Teams/Email/Slack	Output channels	API, webhook	OAuth2/app reg	None for channeling	Logging, data privacy
Data Warehouse	Structured, transactional	JDBC/ODBC/ API	Service acct/IAM	Data mapping, audit log injection	Role-limit, PII
Vector Store	Unstructured docs/ semantic	API/SDK	Service acct/IAM	Chunk/embedding, doc tagging	Role-limit, data vault

Transformation Needs:
- ETL pipelines for all structured sources (account/transaction data), including mapping, deduplication, cross-source validation.
- Automated conversion of all deliverables (Word, PPT, PDF, notes) to vector-friendly formats with document-level embeddings for RAG/search.
- Ensure masking or redaction of PII where not required for use-case.
- Tagging/versioning of all records for compliance audit.
- All access must be logged and retained according to data governance/retention policy.

Actor Setup Responsibilities

Actor Role	Setup Tasks / Responsibilities	Systems/Touchpoints	Actions Required
IT/Security (FinGuard)	Cloud resource provisioning, network access, IAM	Azure/AWS, Key Vault, Subatomic, VMs, storage	Create cloud infra, assign IAM, enforce firewalls, approve integrations
Ops/Back Office	System integration config, template mgmt, agent settings	Subatomic, API connectors, templates/storage	Configure API access, test data flow, update templates
Vendor/AI Provider	Subatomic deployment, integration support	Subatomic, Connector APIs, documentation	Setup/install AI platform, enable connectors, assist testing
System Vendors (Redtail, Black Diamond, etc.)	API key creation, webhook/app reg	Each SaaS (admin/user portal), support desk	Issue credentials, approve API clients, enable webhooks
Paraplanners/Advisors	No technical setup; review outputs, user feedback	UI portal, Teams/Slack, Subatomic UI	Validate output, adjust config via feedback, train
Compliance/Ops (future)	Audit log review, compliance dashboard config	Data Warehouse, Subatomic logs	Monitor audit streams, manage compliance overlays

Setup Objectives and Rationale

Sample Rows:

Setup Requirement	Purpose/Rationale	Business Value	Dependencies
Enable secure API/service account access for all core systems (Redtail, RightCapital, Black Diamond, custodians)	Automate end-to-end data ingestion, reduce manual handling, support AI workflows	Radically accelerates prep time, reduces errors, scalability	API vendor approvals, cloud infra
Provision segmented cloud environment with encrypted storage for vector DB and warehouse	Supports structured and unstructured data pipelines with strict compliance	Enables RAG/semantic AI, analytics, robust compliance	IT/FinGuard resource setup
Credential vault for all integration secrets (Key Vault/ Secrets Manager)	Central, auditable control and rotation of access tokens/keys/passwords	Security, compliance, audit tracing	Cloud infra provisioned
Agent-based modular integration via Subatomic platform	Enables scalable, flexible workflow automation and human-in-loop control	Consistency, future-proofing, process optimization	Core integrations configured
Automated audit log and compliance overlay integration	Regulatory reporting, role- and action-level traceability	Reduces compliance risk, audit cost	Data warehouse, logging enabled

Access and Setup Gap Analysis

Gap Title	Gap Description	Potential Solution	Dependencies	Notes / Blockers
API/API Key Unavailability (Custodian etc.)	Missing modern API or lack of issued credentials from some core systems (e.g., Wealthscape, Schwab)	Request vendor enablement, interim: automate secure file pickup	Vendor/SaaS approval, security review	Key blocker for full automation
Service Account Role/ Permission Issues	Service accounts for AI agents lack least privilege config or are not yet provisioned	Work with IT/ops to scope/ assign per-agent, per-system roles	IAM setup, cloud admin, security policies	Risk of overbroad access
Incomplete Data Flow Mapping/Testing	Field-level gaps or mismatch between source schemas and warehousing vector/ structured layers	Thorough mapping, ETL transformation pipeline, iterative QA	Access to sample data, schema docs	Needs ops/vendor engagement
Audit/Compliance Logging Not Centralized	Action logs/fragments in multiple systems, not unified for agent/audit layer	Develop pipeline for all agent/ system actions into warehouse log	Logging infra, agent instrumentation	Requires business rules codified
Cloud Perimeter/ Networking Unfinalized	Unclear cloud network rules, lack of clear boundaries, possible exposure	Finalize subnets/firewalls, enforce only approved ingress/ egress	IT network/security, cloud policy	Cannot deploy until resolved

Gap Title	Gap Description	Potential Solution	Dependencies	Notes / Blockers
Credential Management Lacking or Manual	Integration secrets or tokens scattered, risk of sprawl/rotation issues	Consolidate to Key Vault/secret manager w/ automation	Cloud infra ready, process/IT ownership	Interim risk if unmanaged
API Rate Limiting or Vendor Quota Block	Some vendors throttle high-frequency API access (batch/real-time ingest)	Negotiate higher quota, implement retry/backoff, batch appropriately	Vendor relationship, rate policy	Scaling bottleneck for real-time
Data Retention/PII Policy Clarity	Some data sources (client, custodian) have unclear retention/redaction policy	Work with compliance to codify/ implement via ETL / agent logic	Compliance/officer engagement	May block DX to warehouse/vector
Output Channel App Registration Pending	MS Teams, Slack, Email integration needs tokenize/app reg + IT approval	IT registers apps, issues API keys	IT admin, Teams/Slack admin access	Partial/manual until provisioned

End of Access and Setup Requirements Model

Report Metadata

Metadata	Value
Client Name	Vantage Financial
Report Type	Access and Setup Requirements Analysis
Generated By	ASRD Definer System
Generation Date	2025-12-03 12:20:00
Access and Setup Requirements	✓ Included

End of Report