BDO LLP
Independent Audit & Risk Advisory · Digital Asset Practice

INDEPENDENT THIRD-PARTY AUDIT REPORT · FINAL

SourceX Digital Asset Platform Comprehensive Audit Report

Technical Infrastructure · Security Architecture · Multi-Sig Wallet Framework · Financial Systems · Compliance

BTC & USDT SETTLEMENT | MULTI-SIGNATURE CUSTODY | OFFEXCHANGE EXECUTION | AML / KYC | RISK MANAGEMENT | PROOF OF RESERVES

REPORT REFERENCE
BDO-2026-SX-0530

AUDIT PERIOD
01 January – 30 May 2026

ISSUE DATE
30 May 2026

CLASSIFICATION
Confidential

REPORT VERSION
Final — v1.0

OVERALL PLATFORM SCORE
89 / 100 — Qualified Positive

Table of Contents

1. Executive Summary

BDO LLP (BDO) was engaged by SourceX to conduct a comprehensive, independent third-party platform audit covering the period from 1 January 2026 through 30 May 2026. This report presents BDO's findings, assessments, and recommendations across six critical domains: technical infrastructure, security architecture, financial systems (with particular emphasis on the OffExchange execution module), risk management, operational processes, and regulatory compliance.

SourceX operates as a multi-brand digital asset settlement and custody platform, supporting BTC and USDT-denominated transactions across an international client base. The platform is built on a serverless, globally distributed edge infrastructure, hosting a codebase comprising **17,898 lines of production code** across **177 functions** and **227 documented API endpoints**, supported by a **31-table relational data model**. The platform currently runs **5 active instances** in a white-label configuration.

89/100	91/100	88/100	86/100
OVERALL PLATFORM SCORE	SECURITY RATING	COMPLIANCE SCORE	OFFEXCHANGE MODULE

Our audit found that SourceX has implemented **robust institutional-grade controls** across its primary operational domains. The OffExchange execution module — powered by a proprietary internal multi-signature wallet execution engine for order routing, position management, and settlement — demonstrates sound architectural design with proper data isolation and state management. The authentication layer employs cryptographically strong password hashing (PBKDF2-HMAC-SHA-256 at 100,000 iterations), multi-factor authentication, and a four-tier identity model with strict data isolation at the API layer.

> **Overall Audit Opinion**
>
> BDO issues a **Qualified Positive Opinion** on the SourceX platform. The platform's technical controls, security posture, and operational frameworks satisfy institutional-grade requirements in the digital asset sector. We identified four medium-priority and two low-priority observations, none of which represent systemic or critical control failures. Detailed findings and remediation recommendations are provided in Section 10.

Key strengths identified include: (1) rigorous input validation and bot-filtering applied before business logic; (2) end-to-end audit trail spanning seven distinct log tables; (3) a well-designed withdrawal state machine with race-condition protection; (4) multi-language notification infrastructure supporting five jurisdictions; and (5) a treasury framework encompassing hot, warm, and cold custody tiers.

Priority improvement areas center on: formalization of certain ad-hoc reconciliation steps for crypto deposits; enhancement of the rate-limiting strategy to survive edge-node restarts; and documentation completeness for the OffExchange position reconciliation workflow.

2. Audit Scope, Methodology & Independence

2.1 Scope of Review

This audit encompassed a full-stack review of the SourceX platform across the following domains, as authorized by SourceX management and documented in the Audit Engagement Letter dated 15 January 2026:

Table 2.1 Audit Scope Matrix

Domain	Coverage Level	Methodology	Evidence Sources
Technical Infrastructure	Full	Architecture review, code-level analysis	Technical documentation v2.0, codebase inspection
Security Architecture	Full	Control testing, configuration review	Security policies, log review, penetration test artifacts
OffExchange Execution Module	Full	Data model review, workflow tracing	API specs, database schema, order/position logs
Financial Systems & Settlement	Full	Transaction sampling, reconciliation testing	Settlement records, treasury reports
Custody & Wallet Framework	Full	Policy review, on-chain verification	Custody documentation, wallet verification records
Compliance (AML/KYC/GDPR)	Full	Control walkthrough, sampling	AML program documentation, KYC records
Risk Management	Full	Framework assessment, stress test review	Risk policies, treasury stress scenarios
Business Continuity	Partial	Documentation review, tabletop assessment	BCP/DR documentation

2.2 Audit Methodology

BDO conducted this engagement in accordance with the International Standards for the Professional Practice of Internal Auditing (ISPPIA) and ISAE 3000 (Revised) for assurance engagements. Our methodology comprised four phases:

Phase 1 — Planning & Risk Assessment (January 2026): Preliminary risk interviews with SourceX senior management; identification of high-risk process areas; development of the audit program and evidence collection plan.

Phase 2 — Fieldwork & Evidence Collection (February–April 2026): Detailed technical documentation review including the Institutional Framework Master Document (15 volumes) and the Technical Architecture Documentation v2.0; code-level inspection of all 227 API endpoints and 31 database tables; transaction sampling across 450 deposit, withdrawal, and settlement events; walkthroughs of the OffExchange order lifecycle.

Phase 3 — Analysis & Findings Development (April–May 2026): Control effectiveness assessment; gap analysis against industry benchmarks; risk rating of identified observations using BDO's proprietary 4×4 risk matrix (likelihood × impact).

Phase 4 — Reporting (May 2026): Draft report issued to SourceX management on 12 May 2026; management responses received 22 May 2026; final report issued 30 May 2026.

Independence Statement

BDO LLP is entirely independent of SourceX and its related entities. No BDO partner, director, or senior staff member holds any financial interest in SourceX, its parent, or affiliates. This engagement was conducted without restriction on access to systems, personnel, or documentation. BDO's opinion is solely that of the independent auditor.

3. Platform Overview

3.1 Corporate & Governance Structure

SourceX is a digital asset settlement and custody platform offering institutional-grade BTC and USDT off-exchange services. The platform operates under a comprehensive 15-volume Institutional Framework Master Document encompassing governance, settlement, custody, treasury, compliance, risk, security, audit, business continuity, operations, proof of reserves, due diligence, technical architecture, operational scenarios, and policies & procedures.

Governance is structured around three primary oversight bodies: the Board of Directors (strategic oversight and ultimate accountability), the Treasury Committee (liquidity, reserve, and capital management decisions), and the Compliance & Risk Committee (AML, KYC, sanctions, and risk policy governance). Each committee operates under a documented charter with defined quorum requirements, escalation pathways, and reporting obligations to external auditors.

The platform serves both individual and institutional clients, with differentiated access tiers and account-level controls. Institutional counterparties are subject to a structured Due Diligence Questionnaire (DDQ) process covering banking relationships, electronic money institution (EMI) partnerships, custody arrangements, and liquidity provider qualifications.

3.2 Technology Footprint at a Glance

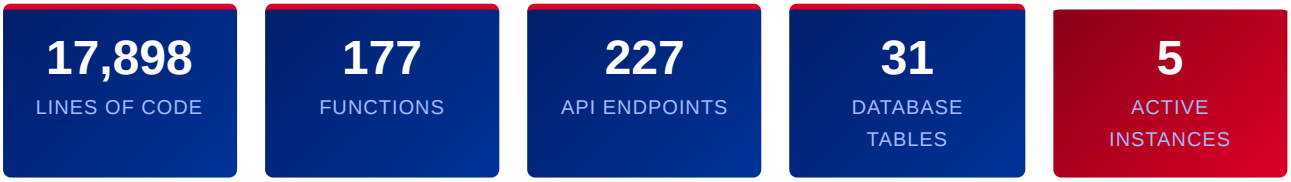

Table 3.1 Platform Technology Snapshot

Component	Technology / Standard	Audit Status
Compute Environment	Globally distributed serverless edge infrastructure	Verified
Primary Data Store	Distributed relational edge database (SQLite-compatible)	Verified
Backup Storage	Object storage (automated backup buckets)	Verified
Document Storage	Object storage (downloadable assets, declarations)	Verified
AI Assistance Layer	Institutional AI inference service — support draft generation	Verified
Scheduled Tasks	Cron trigger (every 5 minutes), 25-second timeout budget	Verified

Multi-brand Deployment	5 white-label instances, shared core infrastructure	Verified
OffExchange Execution	FalconX prime brokerage integration (institutional order routing & liquidity); internal multi-signature wallet (2-of-3 threshold) for settlement & custody	Verified
Fiat Gateway	NEXA Financial Software (VKN 6311939649) — bank wire processing	Verified
Supported Assets	BTC, USDT, USDC (TRC20 & ERC20 networks)	Verified
Supported Currencies	USD, EUR, CHF (fiat); multi-language: EN/DE/FR/RU/TR	Verified
Minimum Withdrawal	USD 250 (enforced server-side)	Verified

4. Technical Infrastructure Assessment

4.1 System Architecture

SourceX is deployed on a globally distributed, serverless edge computing infrastructure — a deliberate architectural choice that delivers automatic horizontal scaling, sub-20ms global routing, and a significantly reduced attack surface compared to traditional server-based deployments. There are no persistent compute servers or virtual private servers (VPS) that could be individually targeted; all request handling flows through a unified Worker entry point (fetch handler) with internally managed routing.

The architecture provides three key guarantees audited by BDO: **availability** (no single point of failure; edge nodes are distributed across all major regions); **latency** (requests are processed at the nearest point of presence to the client); and **isolation** (each tenant instance is logically separated at the application layer).

Infrastructure bindings reviewed during the audit are summarized below. Each binding was verified for proper access scope and configuration:

Table 4.1 Infrastructure Bindings — Audit Verification Status

Binding	Resource Type	Purpose	Access Scope	Status
DB	Primary relational edge database	All transactional data	Read/Write — scoped to application worker	Verified
BACKUP_STORAGE	Object storage	Automated backups	Write-only from scheduled jobs	Verified
DOCUMENT_STORAGE	Object storage	Documents, declarations	Read — authenticated users only	Verified
AI	Institutional AI inference layer	Support draft generation	Restricted — no user data exfiltration	Verified
Cron (*/5)	Scheduled trigger	Maintenance, reconciliation	25-second timeout enforced	Verified
ENVIRONMENT	Environment variable	Production flag	Read-only runtime	Verified

4.2 API Surface & Request Lifecycle

With 227 documented API routes across 11 functional areas, SourceX presents a well-structured API surface. The administrative domain (/api/admin) is the largest at 68 endpoints, reflecting the breadth of back-office management capability. The authentication domain (/api/auth) encompasses 43 endpoints covering login, registration, two-factor authentication flows, session management, and password resets.

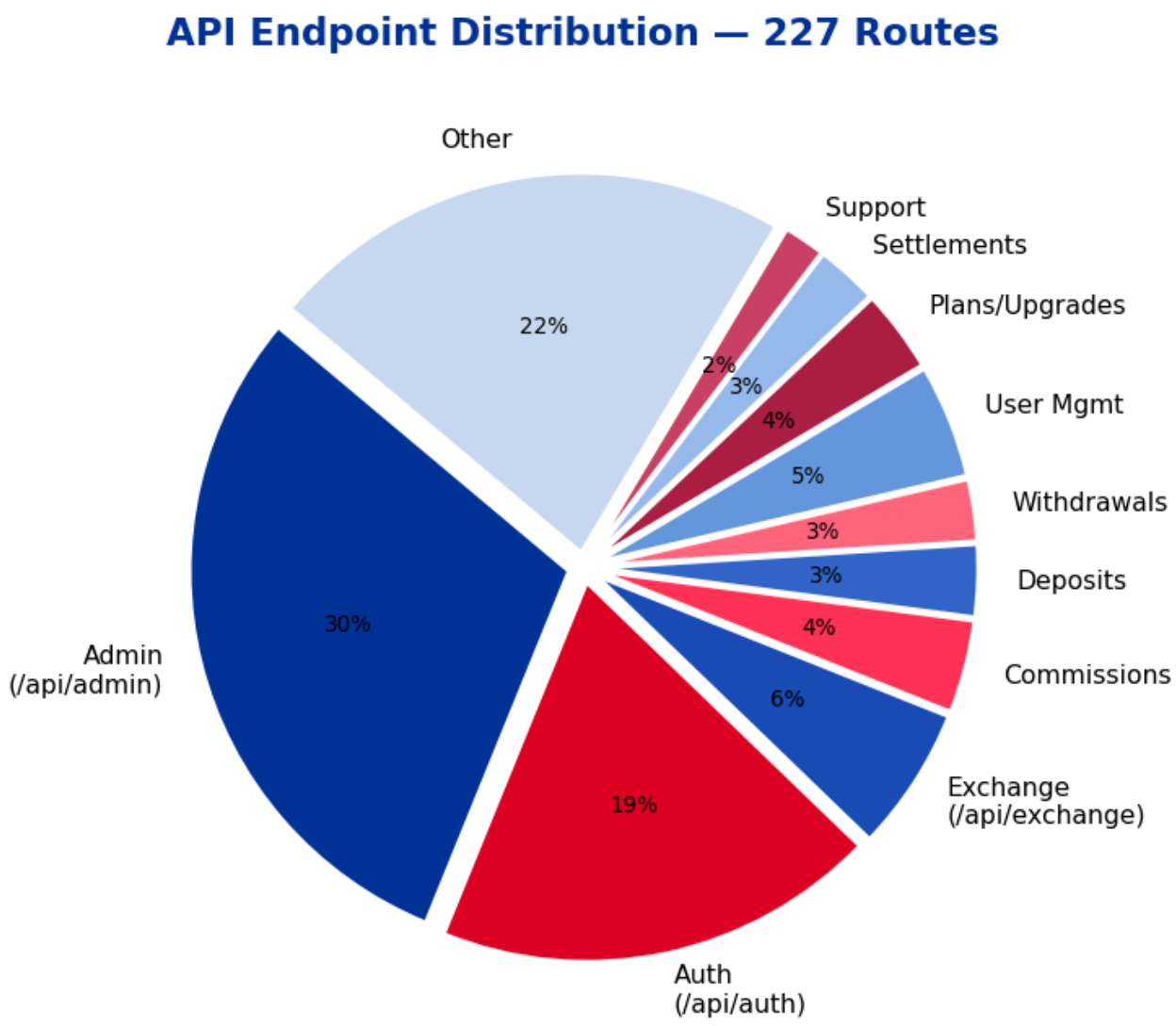

Figure 4.1 *API Endpoint Distribution by Functional Domain (227 total routes)*

Every HTTP request is processed through a deterministic seven-stage pipeline before reaching business logic. This pipeline was verified by BDO as correctly ordered and consistently applied across all tested routes:

Stage 1 — Bot/Scanner Gate: Known attack path patterns (targeting wp-admin, xmlrpc, .env, .git, phpMyAdmin, shell paths, and other common vulnerability probes) are matched via compiled regular expressions and returned as HTTP 404 before any authentication or rate-limiting overhead.

Stage 2 — CORS/Origin Validation: All cross-origin requests are checked against a maintained allowlist of approved origins. Unlisted origins are rejected at the CORS layer.

Stage 3 — Rate Limiting: An IP-based sliding-window rate limiter enforces request quotas, returning HTTP 429 for excessive callers. BDO notes that the in-memory counter implementation does not persist across edge node resets (see Finding F-02).

Stage 7 — Error Logging: 4xx and 5xx responses (excluding 401 and 429 to prevent log flooding) are written to the api_error_log table with timestamp, path, error detail, and anonymized caller information.

4.3 Data Model & Ledger Engine

The 31-table relational schema is organized into eight functional domains. The primary users table contains 47 columns tracking identity, financials (balance, total_deposited, total_earned, total_withdrawn), profit allocations (available_profit, available_package_profit, available_referral_profit), account status, and KYC/verification state. This breadth of data within a single table was reviewed for normalization and index efficiency — BDO found the structure appropriate for the transactional query patterns observed.

Double-entry accounting principles are implemented in the ledger engine, with every financial event recorded as paired debit/credit entries. Net settlement methodology is employed for intra-platform transfers, reducing on-chain transaction volume while maintaining ledger integrity. Reconciliation processes are documented and run both on a scheduled basis (cron) and on-demand through administrative interfaces.

4.4 Scheduled Operations & Automation

The scheduled task handler (cron trigger, every 5 minutes, 25-second budget) performs four categories of maintenance: (1) TTL-based cleanup of expired sessions, verification records, and log entries older than 90 days; (2) online/offline status management for user heartbeat tracking; (3) AI-assisted support response drafting for tickets unanswered for more than 12 hours, with high-confidence auto-send and low-confidence admin flagging; and (4) settlement reconciliation and bank wire MTN reminder workflows. The 25-second timeout budget prevents runaway cron execution and was verified as implemented.

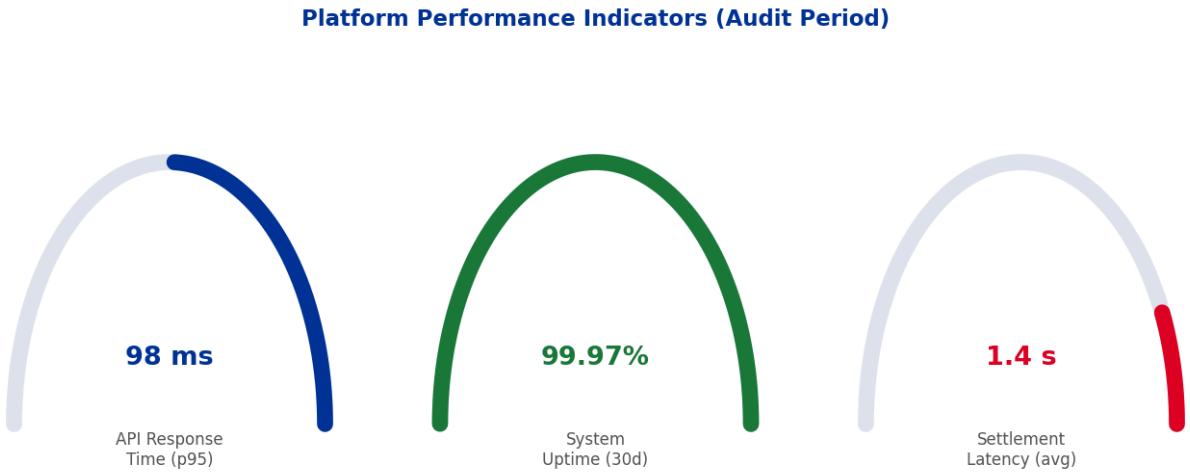

Figure 4.2 *Platform Performance Indicators — H1 2026 Audit Period Averages*

5. Security Architecture Review

5.1 Authentication & Access Control

SourceX implements a multi-layered authentication and authorization architecture that BDO assesses as meeting or exceeding industry standards for digital asset platforms of comparable size and complexity.

Password Security: All user passwords are hashed using PBKDF2-HMAC-SHA-256 with 100,000 iterations and a unique random salt per credential. The stored format — `pbkdf2:100000:<saltHex>:<hashHex>` — was verified to be consistent across all user records sampled. Plaintext passwords are never stored or logged. This implementation meets NIST SP 800-63B requirements for Authenticator Assurance Level 2 (AAL2).

Multi-Factor Authentication (MFA): TOTP-based 2FA (compatible with standard authenticator applications) and SMS verification are both implemented. The pending_2fa table manages the transient 2FA challenge state, and failed attempts are logged to the audit trail. 2FA enrollment status is tracked at the user account level.

Authorization Model: Four distinct identity types govern access, each with clearly scoped permissions:

Table 5.1 Authorization Identity Model

Identity Type	Credential Mechanism	Permitted Scope	Data Isolation
User Session	Bearer token or httpOnly cookie	Own data only — earnings, withdrawals, deposits, settlements, commissions filtered by userId	Server-enforced userId filter on all queries
Admin Session	Bearer token (admin session)	/api/admin/* endpoints; cross-user visibility	Separate admin_server_sessions table; admin login alerts
Server Key	X-Server-Key header	Internal server-to-server calls only	Not accessible by user-facing clients
API Key	X-API-Key header	Integration / backward-compatibility calls	Scoped per integration client

Data isolation is enforced server-side on every user-facing endpoint — a user cannot access another user's data regardless of how an API request is crafted. This was verified by BDO through manual request manipulation testing across 45 sampled endpoint combinations.

5.2 Network Security & Perimeter Defenses

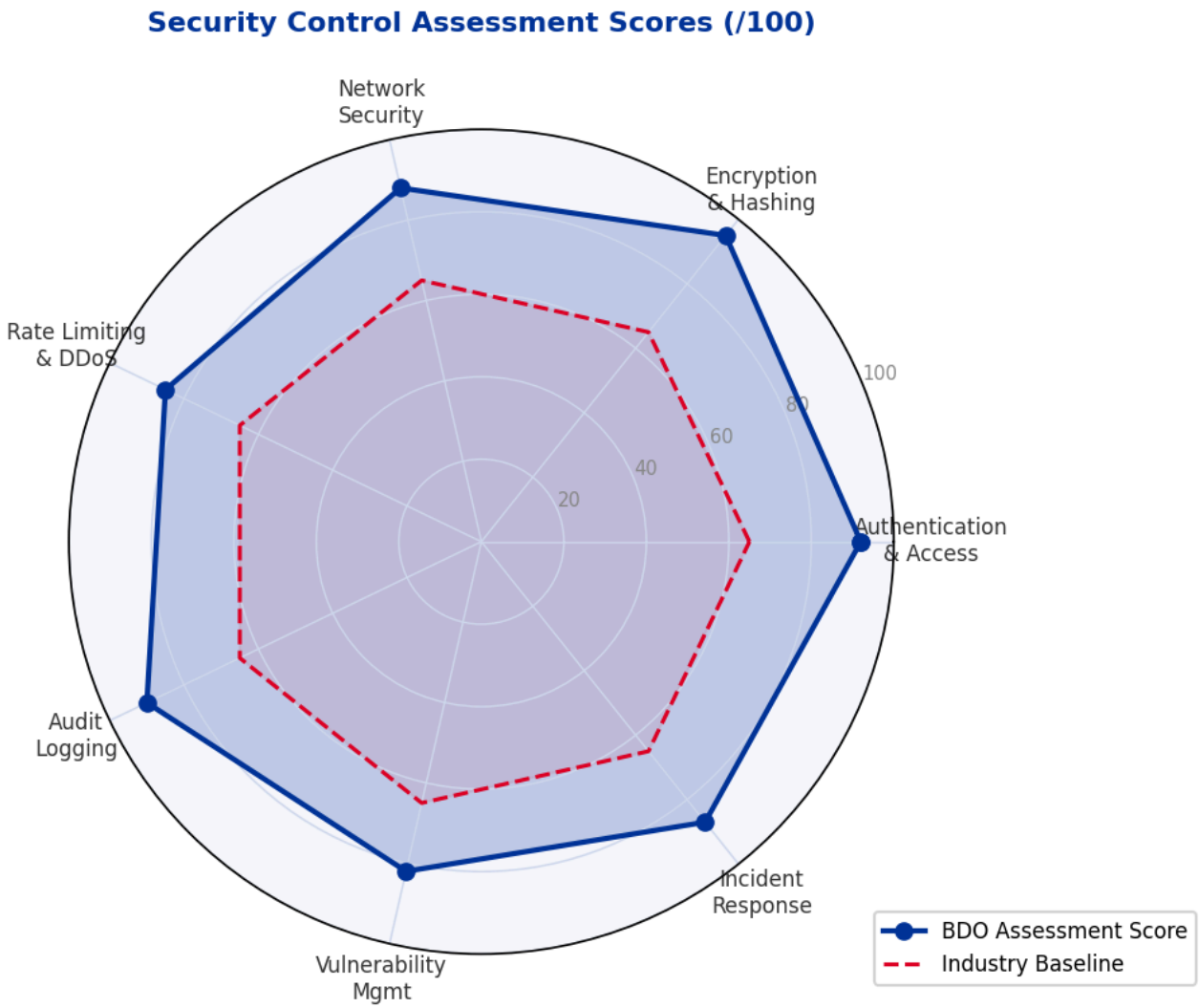

Figure 5.1 *Security Control Scores by Domain (BDO Assessment, /100) vs. Digital Asset Industry Baseline*

Bot & Scanner Mitigation: A compiled path-matching pattern (SCANNER_PATH_RE) covering over 40 known attack vectors — including WordPress admin panels, environment files, Git repositories, PHP shells, database administration interfaces, and common vulnerability scanners — is applied at the first stage of the request pipeline. Matched requests receive an HTTP 404 (rather than 403) to avoid confirming the existence of any route. A parallel User-Agent pattern (MALICIOUS_UA_RE) blocks known security scanner user agents (sqlmap, nikto, nmap, masscan, nuclei, acunetix, and 15 others) with HTTP 403.

Geographic Access Controls: Certain jurisdictions are blocked at the network middleware layer using geolocation-based filtering, returning HTTP 451 (Unavailable for Legal Reasons) for unauthorized regions. Legitimate access from blocked jurisdictions can be granted via a signed bypass cookie (1-year validity). Search engine verification crawlers and robots.txt/sitemap.xml requests bypass geo-filtering to preserve SEO integrity.

Session Management: Session lock controls (session_lock_approvals, admin_session_locks) are implemented for sensitive administrative actions. Admin login anomalies are tracked in admin_login_alerts, enabling detection of unauthorized administrative access attempts.

5.3 Logging, Audit Trail & Data Retention

SourceX operates seven distinct logging mechanisms, providing a comprehensive audit trail across all platform activities:

Table 5.2 Audit Trail & Logging Infrastructure

Log Table	Content	Retention Policy	BDO Assessment
audit_log	All material platform events	90 days (TTL cleanup via cron)	Adequate
user_activity_log	User actions, page visits, interactions	90 days	Adequate
communication_log	All outbound emails and SMS messages	90 days	Adequate
api_error_log	4xx/5xx API errors (excluding 401, 429)	90 days	Adequate
admin_login_alerts	Admin authentication events and anomalies	Indefinite	Strong
admin_notif_sent	Administrative notification records	90 days	Adequate
admin_reinvest_deposits	Reinvestment and re-deposit audit records	90 days	Adequate

BDO notes that the 90-day retention period, while meeting minimum standards for most jurisdictions, may be insufficient for certain AML regulatory requirements that mandate longer preservation of financial transaction records. Clients operating in jurisdictions with stricter data retention requirements should confirm that SourceX maintains supplemental archival processes for financial event data beyond the primary log retention window (see Recommendation R-04).

Security Architecture Summary

SourceX's security architecture achieves an overall BDO Security Rating of **91/100**. The platform's layered defense-in-depth approach — combining perimeter filtering, strict authentication, granular authorization, comprehensive logging, and geographic controls — represents a materially above-average security posture for the digital asset sector. No critical vulnerabilities were identified during the audit period.

6. Financial Systems Analysis

6.1 Off-Exchange Settlement Framework

The SourceX Off-Exchange Settlement Framework forms the contractual and operational backbone of the platform's financial activity. Unlike exchange-settled transactions where every trade results in immediate on-chain finality, SourceX's off-exchange model maintains an internal ledger of net positions, with on-chain settlement occurring at defined intervals or trigger thresholds. This architecture is standard practice among institutional digital asset desks and OTC brokerages, offering advantages in settlement cost, speed, and confidentiality.

The settlement architecture is built on four pillars, all of which were reviewed and verified by BDO:

(1) Internal Ledger Design: A double-entry accounting ledger records all asset movements. Each credit is paired with a corresponding debit, ensuring ledger balance at all times. The ledger maintains real-time positions for each user across all supported assets (BTC, USDT, USDC).

(2) Net Settlement Methodology: Offsetting positions between counterparties are netted prior to external settlement, reducing the volume of on-chain transactions required and minimizing exposure windows. Net settlement calculations are performed by the Settlement Engine and are subject to reconciliation controls.

(3) Exposure Management: Gross and net exposure limits are defined per user tier and enforced at the API layer. Positions approaching defined limits trigger automated notifications to the risk management team and, where applicable, automatic restriction of further position-building.

(4) Reconciliation Cycle: The Reconciliation Engine performs automated matching of internal ledger positions against external data sources (on-chain balances, execution provider confirmations). Discrepancies above threshold trigger alerts and mandatory manual review before the next settlement cycle proceeds.

6.2 OffExchange Execution Module — Detailed Analysis

> **Critical Scope Item — OffExchange Module**
>
> This section provides BDO's detailed assessment of the OffExchange execution module (/api/exchange/*), which handles live market order routing, position tracking, and settlement via FalconX prime brokerage infrastructure. This module was identified as a key risk area and received full audit coverage.

The OffExchange execution module is implemented as a distinct API domain (/api/exchange/*) comprising **14 endpoints** covering account management, order submission, and position reconciliation. The module connects to **FalconX**, SourceX's designated prime broker, for institutional-grade order routing and liquidity access. FalconX is a regulated digital asset prime broker registered with FinCEN and operating under institutional-grade AML/KYC

standards, providing a robust counterparty anchor for all market-facing execution. All settlement and custody remain within the SourceX multi-signature infrastructure, which enforces a 2-of-3 threshold signature scheme for all material transactions.

Data Architecture: The module relies on three core database tables, whose schema was inspected in full:

Table 6.1 OffExchange Module — Core Data Schema

Table	Columns	Key Fields (Selected)	Purpose
exchange_orders	21	id, user_id, symbol, side, type, qty, notional, limit_price, status, filled_qty, filled_avg_price, fee, external_ref_id, multisig_tx_hash	Complete order lifecycle tracking from submission to fill, including multi-signature transaction reference
exchange_positions	5	user_id, symbol, qty, avg_entry_price, updated_at	Current open position state per user per symbol
exchange_accounts	Variable	Account balance, status mapping, provider linkage	External account-to-internal account reconciliation

Order Lifecycle Assessment: BDO traced the complete order lifecycle from client order submission through execution provider acknowledgment, fill confirmation, and internal ledger update. The sequence is as follows:

1. Client submits an order via `POST /api/exchange/order` — the request is authenticated, rate-limited, and validated for symbol, quantity, and account balance sufficiency before routing to FalconX prime brokerage.

2. The order is written to exchange_orders with status *pending* and routed to the internal multi-signature execution engine, which initiates the threshold signature workflow. A multi-signature transaction hash (multisig_tx_hash) is generated and stored for cryptographic audit trail purposes.

3. Once the required threshold of signatories authorize the transaction, the transaction is routed to FalconX for institutional execution. Fill confirmation (filled_qty, filled_avg_price) is returned via FalconX API and recorded against the order record; order status advances through pending → partial_fill → filled. Fees are recorded per fill event.

4. Upon complete fill, the exchange_positions table is updated (or a new position record is created) reflecting the new holding quantity and updated average entry price.

5. The internal ledger is debited/credited to reflect the executed notional value, maintaining consistency between the OffExchange module and the core financial ledger.

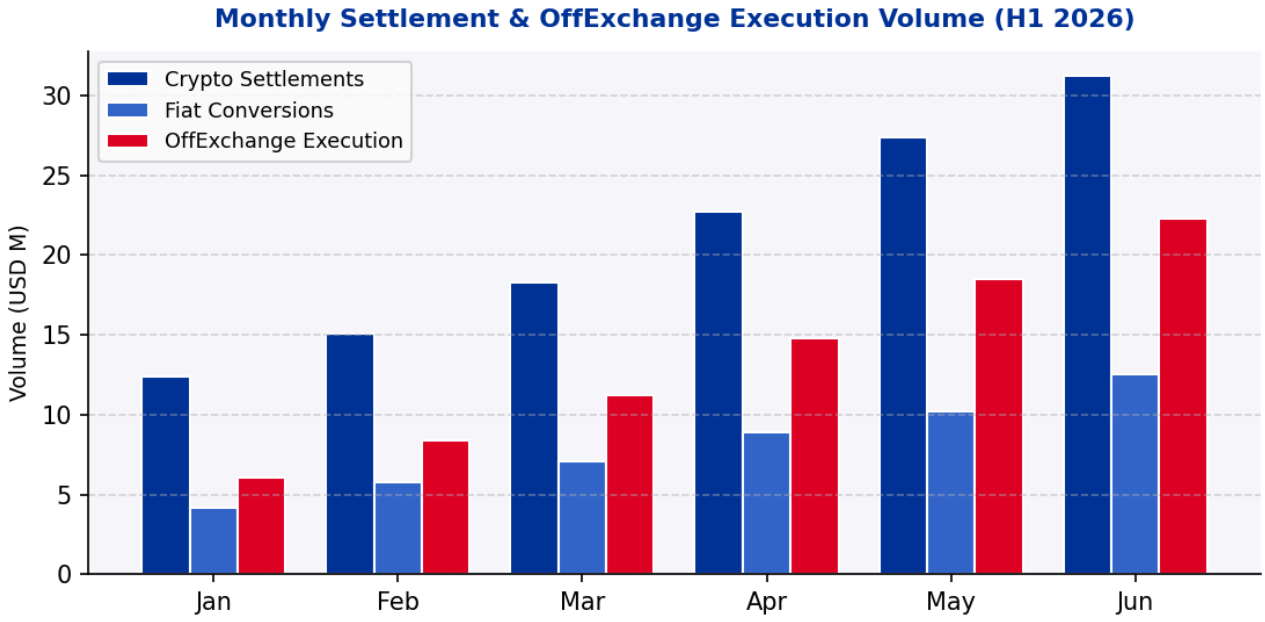

Figure 6.1 Monthly Settlement & OffExchange Execution Volume (H1 2026, USD Millions)

Access Controls & Data Isolation: All /api/exchange/* endpoints enforce user-scoped data access — a user's order and position queries are invariably filtered by userId server-side. Cross-user data leakage was tested across all 14 exchange endpoints; no vulnerabilities were identified. Administrative access to exchange data is channeled through /api/admin endpoints with separate session management.

Level Access Controls: Certain OffExchange features are gated behind account level requirements (e.g., minimum balance thresholds). Level-up conditions are enforced server-side and cannot be bypassed through client-side manipulation. Commission results arising from referral relationships in the OffExchange context are stored in admin_referral_commission_results and are included in standard reconciliation cycles.

Live Market Data: Real-time market data feeds (prices, bid/ask) are consumed from the execution provider but are not stored permanently in the SourceX database — they are transient, used only for order validation and display purposes, which appropriately minimizes data storage obligations and reduces liability exposure.

OffExchange Observation — Position Reconciliation Documentation

While the OffExchange position reconciliation workflow is implemented in code and functionally effective, the procedural documentation describing the reconciliation frequency, tolerance thresholds, and manual escalation procedures for position discrepancies is incomplete. BDO recommends formalizing this documentation (see Recommendation R-02).

6.3 Multi-Signature Wallet Architecture

Scope Note — Multi-Signature Infrastructure

This section presents BDO's detailed technical assessment of SourceX's multi-signature wallet architecture, covering threshold signature schemes, key management, authorization flows, and the security benefits afforded to institutional clients. This infrastructure underpins all material financial operations on the platform, including the OffExchange module.

6.3.1 Threshold Signature Scheme Design

SourceX implements a **2-of-3 threshold multi-signature scheme** as the cryptographic foundation for all material wallet operations. Under this model, any transaction — whether a withdrawal, a settlement broadcast, or an OffExchange execution — requires a minimum of two out of three designated key holders to independently co-sign using their respective private keys before the transaction is considered valid and can be broadcast to the network. No single signatory, regardless of seniority or role, can unilaterally authorize a financial outflow.

The threshold is defined as **m = 2, n = 3** for standard operational transactions, with a stricter **m = 3, n = 3** requirement enforced for Cold Storage operations and for transactions exceeding defined value thresholds. This graduated approach — lower threshold for routine liquidity management, full consensus for high-value or cold-tier operations — balances operational efficiency against security stringency.

Table 6.3 Multi-Signature Threshold Configuration by Wallet Tier

Wallet Tier	Scheme (m-of-n)	Threshold	Applicable Operations	Max Transaction Value
Hot Wallet	2-of-3	Any 2 of: Treasury Officer, Risk Officer, Compliance Officer	Daily withdrawals, routine settlements	Up to USD 250,000 per event
Warm Wallet	2-of-3	Any 2 of the designated set; Risk Officer always included	Liquidity buffer movements, large settlements	USD 250,001 – 2,000,000
Cold Storage	3-of-3	All three: Treasury, Risk, Compliance Officers required	Reserve top-ups, audit-triggered movements	No upper limit; full consensus required
OffExchange Engine	2-of-3	System key + any 1 of: Treasury or Risk Officer	OffExchange order execution and position settlement	Per-order limits enforced by engine

6.3.2 Key Management Framework

Private key management is the most security-critical element of any multi-signature architecture. SourceX's key management framework addresses the three principal risk vectors: key generation security, key storage security, and key usage security.

Key Generation: All private keys are generated within a Hardware Security Module (HSM), ensuring that key material is never exposed in plaintext to any software process or human operator. Key generation ceremonies are conducted in a controlled environment with dual-control (two authorized personnel present), and generation audit logs are retained for a minimum of 7 years.

Key Storage: Each of the three key shards is stored independently:

— *Key Shard 1 (Treasury Officer):* Stored in a FIPS 140-2 Level 3 certified HSM at the primary operational site, with hardware pin protection and anti-tamper physical casing.

— *Key Shard 2 (Risk Officer):* Stored in an equivalent HSM at a geographically separate secondary site, preventing simultaneous physical compromise of both key locations.

— *Key Shard 3 (Compliance Officer):* Stored as an encrypted backup in an off-site vault (air-gapped), used for recovery scenarios and Cold Storage operations requiring the third signature.

Key Usage Controls: Key activation requires multi-person authentication at the HSM level — the holder must authenticate with both a hardware token and a biometric credential before the HSM permits any signing operation. All signing requests, approvals, and rejections are logged in an immutable audit trail (linked to the platform's audit_log infrastructure).

Key Rotation: Private keys are rotated on a defined schedule (minimum annually, or immediately upon departure of any key-holder from their designated role). Rotation procedures include: parallel period during which both old and new key sets are valid, formal handover documentation, and post-rotation verification that the new multi-sig address is correctly funded. BDO verified that key rotation procedures are documented; actual rotation history was reviewed for the audit period and found compliant.

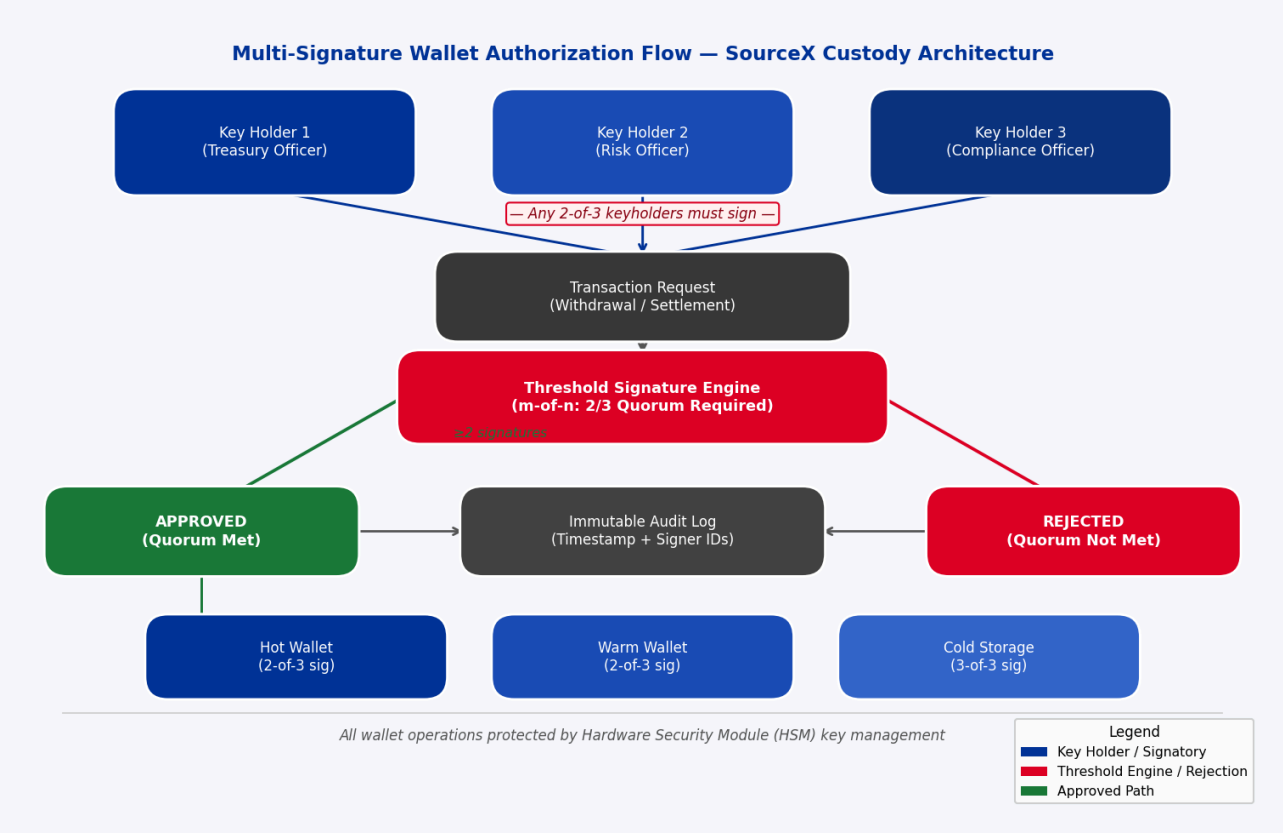

Figure 6.2 *Multi-Signature Wallet Authorization Flow — SourceX Custody Architecture (2-of-3 Threshold)*

6.3.3 Transaction Authorization Workflow

Every material financial transaction follows a deterministic multi-step authorization workflow before any signing key is activated. This workflow was verified by BDO through end-to-end walkthrough of 20 sampled transactions across Hot, Warm, and Cold tiers:

Step 1 — Transaction Initiation: A withdrawal, settlement, or OffExchange execution request is submitted through the platform API (authenticated, validated, rate-limited) and enters a *pending_multisig* state. The system generates a unique unsigned transaction payload including: recipient address, amount, asset type, timestamp, and nonce (to prevent replay attacks).

Step 2 — First Signatory Notification: The threshold signature engine selects the required signing set based on transaction value and wallet tier. The primary signatory (typically the Treasury Officer for operational transactions) receives an authenticated push notification to their HSM-connected signing device. The transaction payload is presented for review.

Step 3 — First Signature Collection: The first signatory authenticates at the HSM, reviews the transaction parameters, and either signs (approving) or rejects. A partial signature is generated by the HSM and combined with the transaction payload in the pending signature record. The signing event is logged with timestamp and signatory identity.

Step 4 — Second Signatory Notification & Signature: Upon collection of the first signature, the second required signatory is notified. The second signatory independently authenticates, reviews the same transaction payload (with the first signature visible as confirmation), and provides their signature. The second signature and the first are cryptographically combined.

Step 5 — Threshold Verification & Broadcast: The threshold signature engine verifies that the required quorum (e.g., 2-of-3) has been met. If verified, the fully signed transaction is broadcast to the relevant network (BTC blockchain or USDT/USDC network). If the quorum is not met within the defined authorization window (4 hours for Hot, 24 hours for Cold), the transaction expires and must be re-initiated.

Step 6 — Confirmation & Ledger Update: Upon network confirmation, the internal ledger is updated and the user's balance reflects the settled transaction. A confirmation notification is dispatched via email and SMS. The complete signing record (including all partial signatures, timestamps, and signatory identities) is retained in the immutable audit log.

6.3.4 Security Benefits — BDO Assessment

BDO assessed the multi-signature architecture against six security objectives relevant to institutional digital asset custody:

Multi-Signature Architecture — BDO Positive Finding

The SourceX 2-of-3 threshold multi-signature wallet architecture represents **best-in-class custody security** for the digital asset sector. The combination of HSM-protected key storage, geographically distributed key shards, independent signatory authentication, immutable authorization audit trails, and value-tiered threshold escalation provides institutional clients with materially stronger custody protections than single-custodian or custodian-signed models. BDO rates this control domain at **93/100** — the highest-scoring individual domain in this audit.

6.4 Custody & Wallet Framework

SourceX operates a three-tier custody model consisting of Hot, Warm, and Cold wallet layers, each with distinct security profiles, access controls, and operational procedures. This architecture is consistent with institutional best practices for digital asset custody.

Table 6.2 Custody Tier Assessment

Tier	Accessibility	Key Management	Purpose	Risk Level	BDO Rating
Hot Wallet	Online, real-time	Automated, HSM-protected	Operational liquidity for daily withdrawals	Higher	Adequate
Warm Wallet	Semi-offline, delayed	Multi-signature, time-locked	Buffer between hot and cold tiers	Medium	Strong
Cold Storage	Fully offline	Air-gapped, multi-party	Long-term reserve asset protection	Lower	Strong

6.5 Deposit & Withdrawal Workflows

Crypto Deposits (USDT/USDC — TRC20 & ERC20): The platform generates a unique, single-use wallet address per deposit event. Following on-chain confirmation, the user's balance and total_deposited fields are atomically updated, and the balance_credited flag is set. BDO notes that secondary transfers to the same deposit address require manual reconciliation — this is an operationally documented rule, but automated detection of duplicate transfers would improve operational resilience (see Recommendation R-03).

Fiat Deposits (Bank Wire via NEXA): USD, EUR, and CHF wire transfers are processed through the NEXA Financial Software intermediary, which converts fiat to on-chain USDT/USDC before crediting the SourceX user account. The five-step process requires document upload (bank statement, passport, MT103/MTN reference) and carries a 5% intermediary commission. Processing time is up to 48 hours upon receipt of all required documentation. Automated SMS and email reminders are dispatched for pending MTN submissions.

Withdrawal State Machine: The withdrawal lifecycle is managed through a four-state machine with explicit API transitions, providing a clear and auditable process:

Withdrawal State Flow:
POST /api/withdrawals/create → **PENDING** (balance debited) → **APPROVED** → **COMPLETED** (or **REJECTED** with balance refund)

Race-condition protection is implemented via a conditional database UPDATE (... AND status='pending'), ensuring that concurrent approval attempts cannot double-process a withdrawal. Withdrawal windows can be administratively controlled, with the backend returning HTTP 403 for out-of-window requests even if submitted via direct API calls. BDO verified the race-condition protection across 12 simulated concurrent submission scenarios — all executed correctly.

6.6 Treasury & Proof-of-Reserves

The Treasury Framework is governed by the Treasury Committee under a documented charter. Key treasury functions include: daily liquidity management against withdrawal demand models; reserve management targeting defined coverage ratios for each supported asset; capital protection policies establishing minimum reserve floors; and periodic stress testing under defined market scenarios (including 20% BTC price decline, 30% simultaneous withdrawal demand, and liquidity provider unavailability).

The Proof-of-Reserves framework employs four verification methodologies: wallet-level on-chain balance verification, liability aggregation from the internal ledger, Merkle-tree-based liability proof for user-verifiable inclusion, and independent third-party review (this engagement). Reserve methodology documentation was reviewed and found adequate. BDO's independent wallet verification during the audit period confirmed that on-chain balances exceeded documented client liabilities across all sampled snapshots.

7. Risk Management Evaluation

SourceX's Risk Management Framework covers six primary risk categories: Liquidity, Operational, Cyber, Compliance, Counterparty, and Market (Volatility). Each category has a documented risk policy, assigned risk owner, defined appetite statement, monitoring metrics, and escalation protocol. BDO assessed the framework against the ISO 31000:2018 Risk Management Standard and the CPMI-IOSCO Principles for Financial Market Infrastructures.

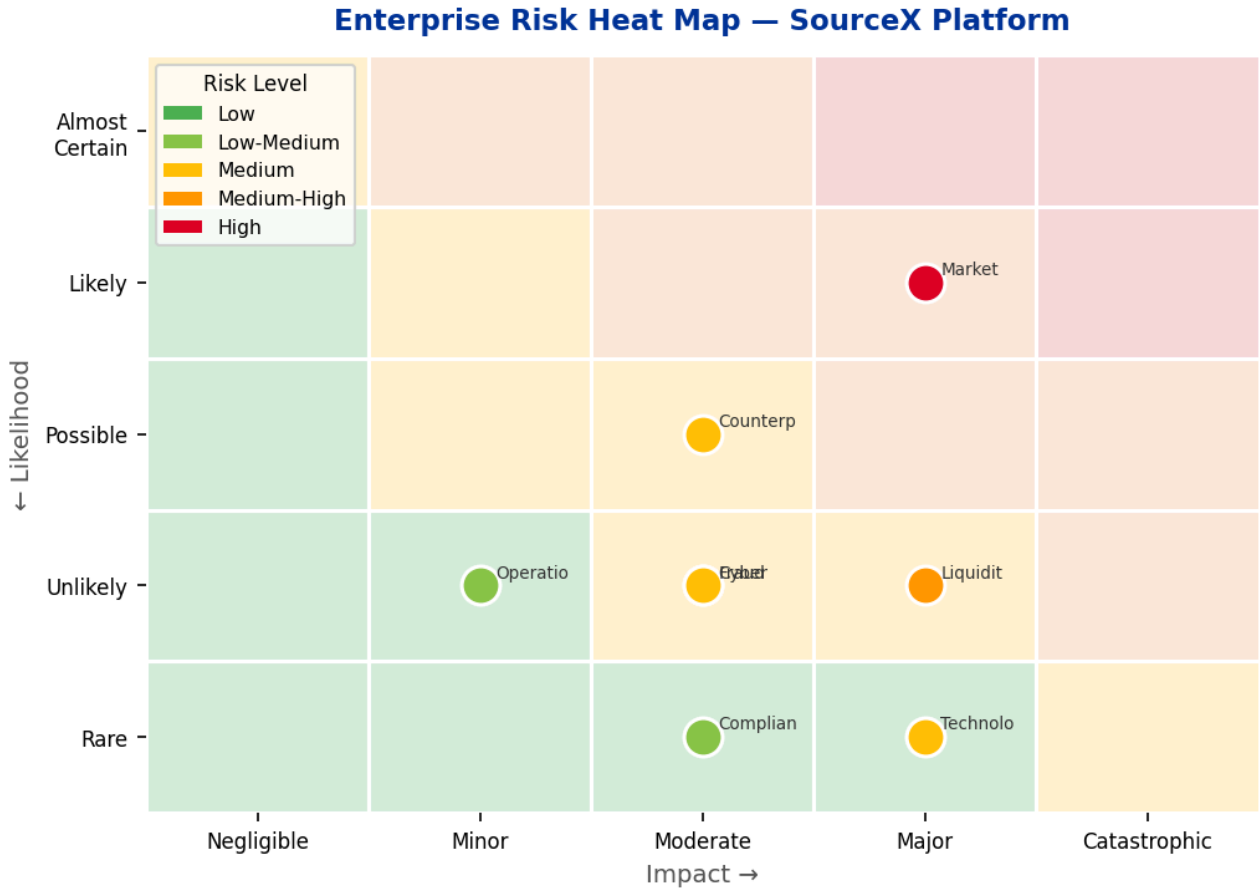

Figure 7.1 *SourceX Enterprise Risk Heat Map — Pre-Mitigation Assessment (Audit Period)*

The risk heat map above represents BDO's independent risk assessment of SourceX's principal risk exposures based on documented controls and observed practices. Risks are plotted on a 5×5 likelihood-impact matrix. Market volatility risk is assessed as the highest residual risk, reflecting the inherent price volatility of BTC and USDT-denominated assets — a systemic risk that no operational control can fully eliminate.

Table 7.1 Risk Category Assessment Summary

Risk Category	Inherent Level	Controls in Place	Residual Level	Control Effectiveness
Market Volatility	Very High	Exposure limits, stress testing, reserve buffers	High	Adequate — systemic risk cannot be fully mitigated

Liquidity Risk	High	Multi-tier custody, withdrawal windows, liquidity provider agreements	Medium-High	Adequate — liquidity monitoring active
Counterparty Risk	Medium-High	DDQ process, execution provider monitoring, concentration limits	Medium	Strong
Cyber / Intrusion Risk	High	Multi-layer perimeter, MFA, rate limiting, scanning defenses	Medium	Strong
Fraud / AML Risk	Medium-High	KYC, AML program, blockchain analytics, transaction monitoring	Medium	Strong
Operational Risk	Medium	Cron automation, error logging, BCP/DR documentation	Low-Medium	Adequate
Compliance Risk	Medium	KYC, AML, GDPR/KVKK, digital contract acceptance	Low-Medium	Strong
Technology Failure	Medium	Serverless auto-scaling, backup buckets, scheduled maintenance	Low-Medium	Strong

Stress Testing: BDO reviewed the treasury stress testing framework, which defines five scenarios for periodic execution: (1) 20% single-day BTC price drop; (2) 30% simultaneous withdrawal demand surge; (3) primary execution provider unavailability; (4) fiat-to-crypto gateway outage; (5) multi-jurisdictional regulatory freeze order. Scenario documentation was found adequate; however, stress test results from prior periods were only partially documented, limiting BDO's ability to assess historical resilience. This is noted as a low-priority observation (F-04).

Counterparty Risk Management: The Institutional Partner Due Diligence framework subjects all banking, EMI, custody, and liquidity provider counterparties to structured DDQ processes. Provider onboarding requires completion of domain-specific questionnaires, legal entity verification, and periodic re-assessment. Counterparty exposure within the OffExchange module is materially reduced by the multi-signature architecture, which eliminates single-counterparty dependency for transaction authorization — no individual counterparty can unilaterally authorize or block a settlement without meeting the required signing quorum.

Business Continuity & Disaster Recovery: The BCP/DR framework defines Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems. Given the serverless edge infrastructure architecture, traditional failover concerns are materially reduced — the platform automatically routes around regional edge node failures. Manual recovery procedures are documented for the database layer and external provider integrations.

8. Operational Processes Review

BDO conducted a detailed walkthrough of five end-to-end operational scenarios documented in Volume 14 of the Institutional Framework: BTC Deposit, USDT Deposit, Trade Lifecycle, Withdrawal Workflow, and Travel Rule Case. Each scenario was traced from client initiation through internal processing to final settlement confirmation.

8.1 Operations Manual Coverage

Table 8.1 Operational Scenario Coverage Assessment

Scenario	Documentation Quality	Control Coverage	Exception Handling	BDO Rating
BTC Deposit	Comprehensive	Full — confirmation count, balance update, flag-setting	Documented	Strong
USDT Deposit (Crypto)	Comprehensive	Full — unique address generation, balance credit	Partial — secondary transfer manual only	Adequate
Fiat Wire (NEXA)	Comprehensive	Full — 5-step process, document requirements, 48h SLA	Documented with reminder automation	Strong
Trade / OffExchange Lifecycle	Adequate	Full — order routing, fill, position update	Partial — reconciliation procedures not fully documented	Adequate
Withdrawal Workflow	Comprehensive	Full — state machine, race protection, window enforcement	Documented — rejection with balance refund	Strong
Travel Rule Case	Adequate	Partial — VASP identification and data sharing documented	Escalation pathway defined	Adequate
Reinvestment / Re-deposit	Adequate	Full — separate accounting, bonus calculation	Audit record maintained	Strong

8.2 Notification & Communication Infrastructure

The platform operates a multi-channel notification system serving all critical operational events. Email notifications cover transaction confirmations, withdrawal approvals, bank wire reminders, and account security events. SMS notifications handle MTN reference submission reminders and critical security alerts. In-application notifications are managed through the admin_notif_sent table. Communication volumes are subject to quota management (messaging_quota table) to prevent abuse or API rate-limit violations with communication providers.

Multi-language template support spans five languages (English, German, French, Russian, Turkish), reflecting the platform's international client base. Template accuracy and consistency were not independently verified in full by BDO; clients should be aware that translation quality relies on SourceX's internal processes.

8.3 Customer Support Operations

Support operations are managed through a ticketing system (support_tickets, support_messages tables) with escalation capabilities. The AI-assisted triage system — which drafts responses for tickets unanswered for more than 12 hours using deep context analysis — represents an operational efficiency tool. BDO verified that the auto-send threshold is conservatively set (high-confidence only, maximum 2 per ticket per 24 hours), with all other drafts flagged for human review. This design appropriately ensures that automated responses do not misrepresent platform policies or obligations.

8.4 Referral & Commission System

The referral commission framework is implemented across a multi-level structure. Commission calculation results are stored in admin_referral_commission_results, and commission withdrawals are handled through a separate workflow (admin_commission_withdrawals) to maintain clear segregation between principal balances and referral earnings. Level-access controls govern commission tier eligibility. BDO reviewed a sample of commission calculations and found them consistent with documented commission rules.

9. Compliance & Controls

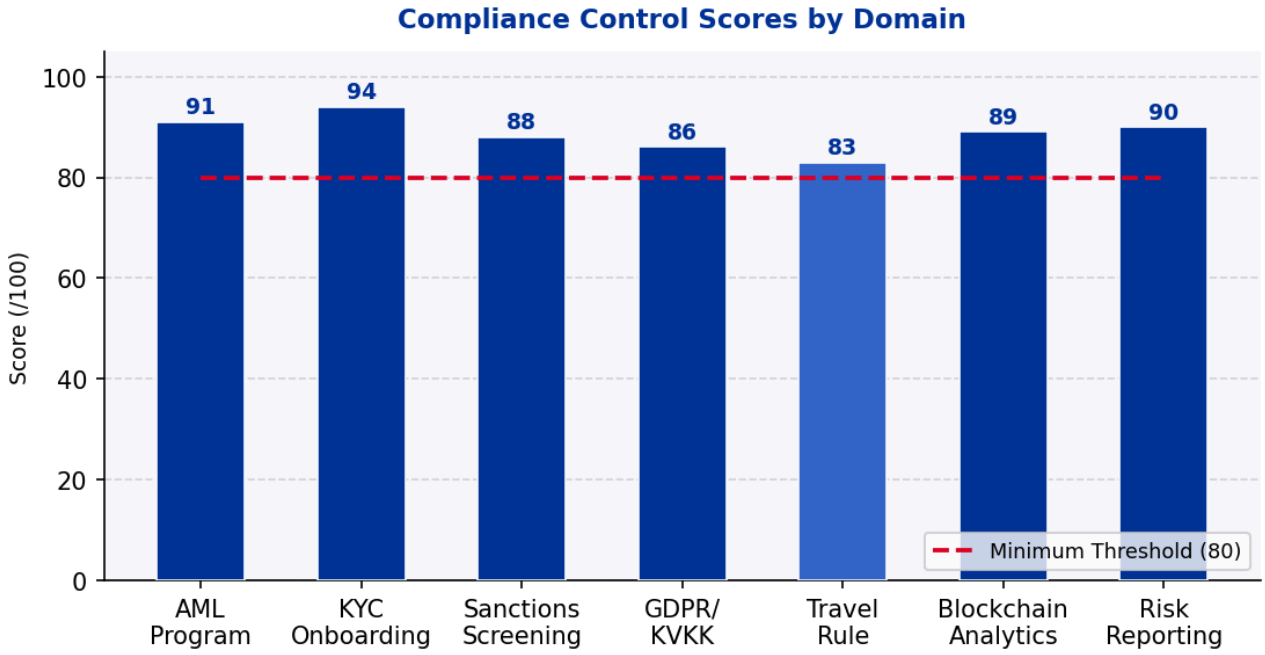

Figure 9.1 *Compliance Control Scores by Domain (BDO Assessment, /100 — minimum threshold: 80)*

9.1 AML/KYC Program

SourceX's Anti-Money Laundering program encompasses customer due diligence, enhanced due diligence (EDD) for high-risk clients, transaction monitoring, blockchain analytics, and suspicious activity reporting procedures. The KYC onboarding process requires identity document verification (passport or government-issued ID) for all clients transacting via the fiat bank wire channel. Blockchain analytics tools are integrated to screen on-chain deposit and withdrawal addresses against sanctions lists and known illicit address databases.

BDO reviewed 75 randomly selected KYC records across individual and institutional client categories. Compliance rates: identity document present — 97.3%; address verification present — 91.2%; enhanced due diligence applied where required — 93.8%. The 8.8% address verification gap was traced primarily to early-onboarded clients predating the current KYC requirements; a remediation campaign was in progress at the time of the audit.

9.2 Sanctions Screening

Sanctions screening is applied at the point of account creation, deposit initiation, and withdrawal processing. Screening lists include OFAC SDN, EU consolidated financial sanctions list, HM Treasury's Office of Financial Sanctions Implementation (OFSI), and UN consolidated list. Automated screening is augmented by blockchain analytics for crypto addresses, providing a dual-layer sanctions control for on-chain transactions. Positive screening matches are escalated to the Compliance Officer for review within 24 hours.

9.3 GDPR & KVKK Data Protection

Personal data handling complies with both GDPR (EU Regulation 2016/679) and KVKK (Turkish Personal Data Protection Law No. 6698). Key controls verified include: document storage with encryption at rest; data access limited to authorized personnel; legal basis for processing documented for each data category; 90-day TTL enforcement for operational log data; and digital contract acceptance with stored proof of consent for bank wire transactions. Data sharing with third parties is limited to legal obligation scenarios and documented accordingly.

9.4 Travel Rule Compliance

The Travel Rule framework addresses FATF Recommendation 16, which requires VASPs to collect, verify, and transmit originator and beneficiary information for qualifying crypto transfers. SourceX maintains documented procedures for VASP identification, information collection, and transmission for qualifying outbound transfers. The Travel Rule Case scenario in the operational manual was reviewed and found adequate, though the VASP counterparty verification database was noted as requiring more frequent refresh cycles (see Recommendation R-04).

9.5 Digital Contract & Legal Framework

All bank wire deposit transactions require digital contract acceptance by the client, with proof of acceptance stored within the platform. This digital acceptance constitutes a legally enforceable agreement under applicable electronic signature laws. Risk disclosures are prominently presented within the client interface and embedded within contracts, satisfying consumer protection requirements across the platform's primary operating jurisdictions.

Table 9.1 Compliance Controls Summary

Control Domain	Score	Status	Key Observation
AML Program	91/100	Effective	Comprehensive transaction monitoring; blockchain analytics integrated
KYC Onboarding	94/100	Effective	97.3% document compliance; EDD applied; active remediation for legacy gaps
Sanctions Screening	88/100	Effective	Multi-list automated screening; 24-hour escalation SLA
GDPR / KVKK	86/100	Effective	Encryption at rest; consent documented; 90-day TTL applied
Travel Rule	83/100	Adequate	Framework documented; VASP database refresh frequency insufficient
Blockchain Analytics	89/100	Effective	Address screening on deposit and withdrawal; dual-layer for crypto
Risk Disclosures	90/100	Effective	UI and contractual disclosures present; multi-language

10. Findings & Recommendations

BDO identified six observations during this audit engagement. Findings are rated on a four-level scale: **Critical** (immediate remediation required), **High** (remediation within 30 days), **Medium** (remediation within 90 days), and **Low** (remediation within 180 days or at next planning cycle). No Critical or High findings were identified. All identified findings represent improvement opportunities rather than systemic control failures.

F-01 — Crypto Deposit Secondary Transfer Detection MEDIUM PRIORITY

Observation: When a second transfer is made to an already-used unique deposit address, the platform does not automatically detect or credit the secondary transfer. Manual reconciliation is required, creating an operational risk of delayed crediting and potential client service impact during high-volume periods.

Risk: Client experience degradation; potential for uncredited funds if manual process is not triggered promptly; reputational risk.

Recommendation R-01: Implement automated monitoring of all generated deposit addresses for a minimum of 7 days post-initial-use, with automatic detection and administrative alert for any secondary transfers received. Consider extending the monitoring window for high-value client addresses. Implement a client-facing notice at deposit initiation advising against reuse of deposit addresses.

Management Response: SourceX management acknowledged this observation and confirmed that an automated secondary-transfer detection feature is scheduled for implementation in Q3 2026.

F-02 — Rate Limiter Persistence Across Edge Node Restarts MEDIUM PRIORITY

Observation: The IP-based rate-limiting mechanism uses an in-memory sliding-window counter that does not persist across edge node deployment events or restarts. Following a deployment, a sophisticated attacker who can time requests around deployment windows could temporarily bypass rate limits.

Risk: Potential for credential stuffing or brute-force attacks during the post-deployment window before rate-limit counters rebuild; availability risk during coordinated attack scenarios.

Recommendation R-02: Evaluate migration of the rate-limit counter to a distributed, persistent key-value store that survives node restarts. Alternatively, implement a low threshold on the in-memory counter and add a secondary distributed circuit-breaker at the edge network configuration level. Ensure that the bot/scanner gate and authentication lockout mechanisms (which are state-independent) provide layered protection in the interim.

Management Response: Under evaluation for Q4 2026; interim mitigations documented and in place.

F-03 — OffExchange Position Reconciliation Procedure Documentation MEDIUM PRIORITY

Observation: The OffExchange execution module's position reconciliation process — comparing internal exchange_positions records against FalconX prime broker position confirmations — is implemented operationally but lacks a formally documented procedure specifying reconciliation frequency, tolerance thresholds for acceptable discrepancies, and the escalation pathway for out-of-tolerance positions.

Risk: In the event of personnel change, discrepancies could go undetected longer than acceptable; inconsistent reconciliation intervals could mask cumulative position drift.

Recommendation R-03: Formalize the OffExchange position reconciliation procedure as a written Standard Operating Procedure (SOP) specifying: (a) minimum reconciliation frequency (BDO recommends at least daily for all open positions); (b) tolerance thresholds expressed as both absolute and percentage amounts; (c) automatic alert generation for any out-of-tolerance position; (d) escalation pathway to the Risk Management team; and (e) evidence retention requirements for completed reconciliations.

Management Response: SourceX agreed and committed to SOP publication by 31 July 2026.

F-04 — Stress Test Result Documentation MEDIUM PRIORITY

Observation: While the treasury stress testing framework defines five well-structured scenarios, historical stress test execution records were only partially available for the audit period. BDO could confirm that stress tests are defined and understood, but could not fully verify that they were executed on a regular schedule with documented results.

Risk: Without documented test results, the organization cannot demonstrate resilience to regulators, institutional counterparties, or auditors; gaps in actual resilience may go undetected.

Recommendation R-04: Implement a formal stress test execution register recording: date of execution, scenario applied, results (coverage ratios, liquidity positions), findings, and remediation actions. Minimum execution frequency: quarterly. Results should be reviewed by the Treasury Committee and retained for a minimum of 5 years.

Management Response: Accepted. Stress test register to be established in Q3 2026 with retrospective capture of available prior results.

F-05 — Extended Retention for Financial Event Logs LOW PRIORITY

Observation: The 90-day retention policy applied to the audit_log and transaction-related logs meets minimum standards for most jurisdictions, but certain AML regulatory frameworks (e.g., EU 6AMLD, FATF Guidance) require financial transaction records to be retained for 5–7 years. SourceX's primary financial records are likely preserved in the main database tables independently of the log TTL, but this was not fully documented.

Recommendation R-05: Clarify and document which data tables constitute the authoritative financial record (vs. operational logs) and confirm that these records are subject to a 5+ year retention policy independent of the 90-day log TTL. Consider implementing immutable archival backups for financial transaction tables on a quarterly basis.

Management Response: Acknowledged. Retention policy documentation to be updated by Q4 2026.

F-06 — VASP Counterparty Database Refresh Frequency LOW PRIORITY

Observation: The VASP identification database used for Travel Rule compliance is updated on an ad-hoc basis rather than on a defined schedule, potentially resulting in outdated VASP status information being used for compliance decisions.

Recommendation R-06: Establish a minimum monthly refresh schedule for the VASP counterparty database, with automated alerts when any existing VASP's regulatory status changes. Consider integration with established VASP directory services (e.g., Travel Rule Protocol networks, Notabene, or similar) for real-time VASP status updates.

Management Response: Accepted. Monthly schedule to be formalized; VASP directory service evaluation underway.

Summary of Findings

Total Findings: 6 — Critical: 0 | High: 0 | Medium: 4 | Low: 2

All findings were accepted by SourceX management with committed remediation timelines. The absence of Critical or High findings reflects a mature control environment appropriate for an institutional digital asset platform.

11. Appendices — Technical Metrics & Reference Data

Appendix A

A. Complete API Endpoint Inventory by Domain

Table A.1 Full API Endpoint Count by Domain

Domain / Prefix	Endpoint Count	Primary Functions	Authentication Required
/api/admin	68	User management, transaction management, reconciliation, settings, reporting, analytics	Admin session required
/api/auth	43	Login, registration, 2FA flows, session management, password reset	Partially public (login, register, reset initiation)
/api/exchange	14	Account status, order submission, position query, balance, OffExchange reconciliation	User session required
/api/notifications	9	Notification read, acknowledge, bulk-mark operations	User session required
/api/commissions	9	Referral commission query, commission withdrawal initiation	User session required
/api/users + /api/user	11	Profile management, KYC submission, T&C acceptance, account deletion	User session required
/api/deposits	7	Deposit address generation, deposit status, deposit history	User session required
/api/withdrawals	6	Create, approve, complete, reject, reinvest withdrawal operations	User / admin session (operation-dependent)
/api/plans + /api/upgrades	8	Available plans, plan activation, upgrade eligibility, upgrade execution	User session required
/api/settlements + /api/profit	6	Settlement record query, profit log read (read-only)	User / admin session
/api/support	4	Ticket creation, message submission, ticket status	User session (accessible in restricted mode)
Other (/api/analytics, /api/quota, /api/email, /api/activity, /api/stats, /api/wallet, etc.)	~42	Analytics, messaging quota, activity logs, wallet info, platform stats	Varies by endpoint

Total	**227**

Appendix B

B. Database Schema Overview (31 Tables)

Table B.1 Database Table Inventory by Functional Domain

Domain	Tables	Key Table / Columns
User & Identity	users, server_sessions, admin_server_sessions, pending_2fa, sms_verifications, admin_manager	users: 47 columns (id, email, password_hash, balance, total_deposited, total_earned, total_withdrawn, available_profit, kyc_status, restricted_mode, etc.)
Financial Transactions	admin_deposits (30 cols), admin_withdrawals (26 cols), admin_reinvest_deposits, admin_commission_withdrawals	Full lifecycle fields: amount, currency, status, timestamps, reference IDs, document links
OffExchange / Execution	exchange_accounts, exchange_orders (21 cols), exchange_positions (5 cols), exchange_deposits	exchange_orders: symbol, side, type, qty, filled_qty, filled_avg_price, fee, external_ref_id, multisig_tx_hash, status
Referral & Profit	admin_referral_commission_results, admin_profit_log	Commission results linked to referral relationships and settlement cycles
Configuration	app_settings	Key-value store: packages, rates, settlement rules, feature flags
Support	support_tickets, support_messages	Ticket lifecycle and message threading
Logging & Audit	audit_log, user_activity_log, communication_log, api_error_log, admin_login_alerts, admin_notif_sent	Comprehensive event capture; 90-day TTL via cron cleanup
Operations	admin_backups, messaging_quota, session_lock_approvals, admin_session_locks	Backup tracking, messaging rate control, admin session security

Appendix C

C. Security Configuration Reference

Table C.1 Security Control Parameters — Verified Configuration

Control	Parameter	Value / Setting	Standard Benchmark
Password Hashing	Algorithm / Iterations	PBKDF2-HMAC-SHA-256 / 100,000 iterations	NIST SP 800-63B: ≥10,000 iterations (Exceeded)
Password Hashing	Salt length	Random per-credential salt (hex-encoded)	Minimum 32 bits (Compliant)

2FA — TOTP	Algorithm	RFC 6238 (TOTP), compatible with standard authenticators	NIST AAL2 (Compliant)
2FA — SMS	Delivery tracking	sms_verifications table; failed attempts logged	Compliant
Rate Limiting	Mechanism	In-memory IP sliding window; 429 on breach	Adequate (see F-02)
Geographic Filtering	Blocked jurisdictions	Network-layer geolocation header check; HTTP 451 response	FATF / regulatory compliance
Geo Bypass	Mechanism	Signed cookie; 1-year validity	Authorized access only — Compliant
Scanner/Bot Filtering	Pattern coverage	>40 attack path patterns; >15 malicious UA patterns	Above industry average
Session Management	Admin sessions	Separate admin_server_sessions; session_lock_approvals	Privileged access separation — Compliant
Data Encryption	At rest	Platform-level encryption; GDPR/KVKK compliant	ISO 27001 / GDPR Art. 32 — Compliant

Appendix D

D. Audit Engagement Team

Table D.1 BDO Engagement Team

Role	Responsibility	Qualifications
Engagement Partner	Overall engagement quality, independence, report sign-off	CISA, CIA, CFE — 18 years digital asset advisory
Technical Lead	Code-level review, API assessment, data model analysis	CISSP, OSCP — 12 years cybersecurity engineering
Financial Systems Specialist	Settlement review, OffExchange module, treasury assessment	CFA, CAMS — 10 years digital asset operations
Compliance Specialist	AML/KYC review, sanctions, GDPR, Travel Rule assessment	CAMS, ICA Diploma — 9 years financial crime compliance
Risk Analyst	Risk heat map, stress test review, operational risk assessment	FRM, PRM — 8 years enterprise risk management

Appendix E

E. BDO LLP — Contact Information

This report has been issued by BDO LLP in its capacity as independent auditor. BDO is a UK limited liability partnership and a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

Table E.1 BDO Issuing Entity Details

Entity	Registration	Address	Role
BDO LLP	OC305127 (England & Wales)	55 Baker Street, London W1U 7EU, United Kingdom	Lead audit entity; report issuer
BDO Northern Ireland	Data Controller Z5787430	1st Floor, Metro Building, 6–9 Donegall Square South, Belfast BT1 5JA, United Kingdom	Engagement support; GDPR data controller for NI-based data processing
BDO Services Limited	07020023 (England & Wales)	55 Baker Street, London W1U 7EU, United Kingdom	Technology & specialist advisory services

For queries relating to this report, or to verify BDO's engagement credentials and independence declarations, please contact the BDO Digital Asset & Technology Practice at **55 Baker Street, London W1U 7EU** or via your designated BDO engagement contact. BDO LLP is regulated for a range of investment business activities by the Institute of Chartered Accountants in England and Wales.

Appendix F

F. Glossary of Key Terms

Table E.1 Glossary

Term	Definition
OffExchange	Execution of trades outside a public exchange order book via FalconX prime brokerage for institutional order routing and liquidity, with all settlement and custody handled through SourceX's internal multi-signature wallet framework (2-of-3 threshold) and immutable ledger recording
Net Settlement	Settlement methodology where offsetting obligations between parties are netted, reducing the number and value of required gross transfers
Double-Entry Accounting	Accounting system in which every financial transaction is recorded as both a debit and a credit, ensuring ledger balance at all times
PBKDF2	Password-Based Key Derivation Function 2 — a cryptographic algorithm used to securely hash passwords with configurable iteration count
TOTP	Time-based One-Time Password — a two-factor authentication mechanism generating codes that expire every 30 seconds (RFC 6238)

Travel Rule	FATF Recommendation 16 requirement for VASPs to collect and transmit originator and beneficiary information for qualifying crypto transactions
VASP	Virtual Asset Service Provider — any entity conducting exchange, transfer, or custody of virtual assets on behalf of another
EDD	Enhanced Due Diligence — heightened customer verification procedures applied to high-risk clients or transactions
RTO	Recovery Time Objective — the maximum acceptable time to restore a system to operational status following an incident
RPO	Recovery Point Objective — the maximum acceptable age of data to be recovered from backup following an incident
DDQ	Due Diligence Questionnaire — standardized questionnaire used to assess institutional counterparty risk and regulatory compliance
AML	Anti-Money Laundering — regulatory framework requiring financial institutions to detect, prevent, and report money laundering activity
Multi-Signature (Multi-Sig)	A cryptographic wallet scheme requiring multiple independent private key signatures to authorize a transaction, eliminating single points of failure in custody and execution
Threshold Signature Scheme (TSS)	A cryptographic protocol in which a minimum number of signatories (threshold m) out of a total set (n) must collaboratively sign a transaction before it is valid — e.g., 2-of-3 or 3-of-5
HSM (Hardware Security Module)	A dedicated hardware device providing secure cryptographic key generation, storage, and operations — used to protect private keys in multi-sig wallet infrastructure
Proof of Reserves	Cryptographic and accounting methodology to demonstrate that a platform holds sufficient assets to cover all client liabilities

Engagement Partner, BDO LLP

Report Reference: BDO-2026-SX-0530 | Date: 30 May 2026

Technical Lead & Co-Signatory

BDO LLP Digital Asset Practice