sera.cx

CONFIDENTIAL — INSTITUTIONAL COUNTERPARTIES ONLY

SERA COMPLIANCE FRAMEWORK · V1.0

Compliance Documentation *for Institutional Counterparties.*

Wallet screening, non-custodial architecture, sanctions and illicit-flow controls, counterparty assurances for institutional liquidity providers, and the protocol-level enforcement model.

DOCUMENT VERSION	ISSUED	ISSUER
1.0	28 April 2026	Sera Compliance

§ 00 · DOCUMENT CONTROL

Document control *and distribution.*

This document is the master compliance reference for institutional counterparties of Sera Protocol. It supersedes any prior compliance summary issued before the date of issue noted on the cover.

Classification

This document is classified **Confidential — Institutional Counterparties Only**. It is intended for sharing with regulated institutional counterparties, their compliance officers and legal advisers, and bona fide due-diligence reviewers, under non-disclosure terms where applicable. Redistribution outside of these audiences requires written permission from the Sera Compliance Function.

Version history

VERSION	DATE	AUTHOR	NOTES
1.0	28 Apr 2026	Sera Compliance	Initial release of the consolidated compliance framework documentation for institutional counterparties.

Document ownership and review

Sera Compliance is the owner of this document and is responsible for its accuracy, currency and distribution. The document is reviewed at minimum on a quarterly cadence, and additionally upon any material change to Sera's compliance posture, regulatory environment, or technical implementation.

Verification of currency

The most recent published version of this document is hosted at `https://sera.cx/compliance`. Recipients are encouraged to verify version currency against the hosted copy before relying on this document for due-diligence purposes. Material changes to the compliance posture between scheduled reviews will be communicated to qualified counterparties through their established compliance contact channel.

Limitations of this document

This document describes the compliance controls Sera operates as a non-custodial protocol. It is not a substitute for the recipient's own legal, regulatory, tax, and compliance analysis. Sera makes no representation that use of the protocol satisfies any specific regulatory requirement applicable to the recipient. Recipients should consult their own counsel for jurisdiction-specific advice.

§ 00 · CONTENTS

Contents.

This document is structured in eleven numbered sections, ordered to take a compliance reader from regulatory posture through architecture to operational details and references.

§ 01 · EXECUTIVE SUMMARY

Executive summary.

A ninety-second overview for compliance officers reviewing Sera as a counterparty. Each point below is expanded in subsequent sections.

What Sera is

Sera is an on-chain foreign-exchange settlement protocol for stablecoins. It is a set of audited smart contracts, deployed on Ethereum mainnet, paired with off-chain quoting and routing infrastructure. Sera does not take custody of user funds at any point; deposits sit in the Vault contract under the depositor's address until withdrawn or settled.

Regulatory posture

Sera is not a licensed money services business, money transmitter, virtual-asset service provider, broker-dealer, or financial institution in any jurisdiction. The protocol is operated as a non-custodial public-good infrastructure layer. Counterparties are responsible for their own regulatory posture under the laws applicable to their activities. The compliance controls described in this document are operated voluntarily.

What this document describes

Sera operates a protocol-level compliance gate that screens every interacting wallet against multi-jurisdiction sanctions lists and illicit-flow typologies. Screening is performed continuously through industry-leading on-chain analytics partners using both Know Your Transaction (KYT) and Know Your Address (KYA) approaches. Non-compliant addresses are denied access at both the application layer (front end and API) and the contract layer (swap router, intent settlement, marketplace).

Why this matters for counterparties

For institutional liquidity providers, this means counterparty flow has been pre-screened by the time it reaches your liquidity. For regulators and reviewers, it means Sera maintains a defensible posture against facilitating sanctioned activity and recognised illicit-flow typologies, while preserving the non-custodial property that is core to the protocol's design.

KEY FACTS AT A GLANCE

Custody model	Non-custodial. Smart contract holds deposits; depositor retains full control.
Smart-contract audit	CertiK, full surface coverage, with continuous monitoring.
Screening cadence	Continuous, pre-trade and intra-trade. Re-evaluation at every interaction.
Screening framework	KYT (real-time monitoring) and KYA (wallet-level risk scoring).
Sanctions coverage	OFAC SDN, EU consolidated, UN, UK HMT, plus comprehensively sanctioned jurisdictions.
Enforcement layer	Application layer (UI, API) and contract layer (router, intent, marketplace).
Funds custody guarantee	`emergencyWithdraw()` callable by any depositor, regardless of access status.
Document classification	Confidential — Institutional Counterparties Only.

§ 02 · REGULATORY POSTURE

Regulatory posture.

Sera operates as an unlicensed, non-custodial protocol. This section makes that posture explicit, identifies what Sera is and is not, and clarifies the boundaries of counterparty responsibility.

What Sera is not

Sera is **not** a licensed entity in any jurisdiction. Specifically, Sera is not registered or licensed as any of the following:

01 **A money services business or money transmitter**
under U.S. federal or state regimes, including FinCEN registration and state-level money transmitter licensing.

02 **A virtual-asset service provider (VASP)**
under FATF, MiCA, Singapore PSA, Hong Kong VASP, or any equivalent regional regime.

03 **A broker-dealer, investment adviser, or exchange**
under U.S. securities laws or any equivalent securities regime in any jurisdiction.

04 **A bank, credit institution, or e-money issuer**
under any banking, deposit-taking, or e-money regulatory regime.

05 **A payment institution or payment service provider**
under PSD2, U.S. payment regulations, or any equivalent payments regime.

What Sera is

Sera is a set of audited smart contracts deployed on Ethereum mainnet, paired with off-chain quoting, routing, and screening infrastructure. The protocol facilitates permissionless cross-stablecoin foreign-exchange settlement. Sera does not take custody of user funds, does not act as a counterparty to swaps, and does not hold or manage client assets in any capacity.

Counterparty responsibility

Counterparties — including institutional liquidity providers, integrators, and end users — are responsible for their own regulatory posture under the laws applicable to their activities. This includes, where applicable: business licensing and registration, customer identification and verification (KYC), source-of-funds documentation, transaction reporting, tax reporting, and compliance with sanctions and AML regimes in the counterparty's jurisdiction. Sera makes no representation that use of the protocol satisfies any specific regulatory requirement applicable to a counterparty's activities.

Why Sera operates compliance controls anyway

Although Sera is not a regulated entity, the protocol operates voluntary compliance controls because: (i) the team takes seriously the risk of facilitating sanctioned or illicit activity through any infrastructure layer; (ii) institutional counterparties require defensible counterparty-screening assurances regardless of Sera's own license status; and (iii) the protocol's long-term integrity depends on its routing graph being free of attributed illicit flow. The controls described in this document are operated on this voluntary basis, not in satisfaction of any specific regulatory mandate.

IMPORTANT — READ IN CONJUNCTION WITH COUNSEL

This document describes Sera's compliance posture and controls. It does not constitute legal, regulatory, tax, or compliance advice. Recipients are responsible for engaging qualified counsel in their own jurisdiction(s) to assess whether their use of Sera meets the regulatory requirements applicable to their activities.

§ 03 · COMPLIANCE ARCHITECTURE

Compliance architecture.

Sera enforces sanctions screening and illicit-flow filtering at the protocol layer. Every wallet that interacts with the protocol passes a compliance gate before any quote is bound or any route is built. Non-compliant wallets are rejected at the contract layer — not merely hidden in the user interface.

The three enforcement points

Compliance is enforced at three logically distinct points in the request lifecycle. Each point is independently configured, monitored, and auditable.

01 **Pre-trade — address screening before quote**

Every connecting address is evaluated against the consolidated blocklist before any route is built or any binding quote is issued. Sanctioned, mixer-linked, hack-attributed, and high-risk addresses never receive a binding quote from Sera. This check sits at the API entry point and is mirrored at the contract entry point.

02 **Intra-trade — continuous re-evaluation**

Wallets are re-screened on a continuous cadence, not only at first connect. New entity attributions and updated risk scores propagate to the gate without operator intervention. If a previously cleared wallet is flagged after onboarding, access is revoked at the next interaction.

03 **Contract-layer enforcement**

The blocklist is enforced not only at the front end and API, but also at the swap router, intent settlement contract, and marketplace contracts. An address that is denied at the application layer is also denied at the contract layer. Bypassing the user interface does not bypass the screen.

Process flow

The diagram below shows the path of a request through the compliance gate. A connecting address first passes through the Compliance Checks gate. If the address clears, the request proceeds to one of two execution paths: rate quoting and swap execution (top branch) or marketplace and limit-order liquidity matching (bottom branch). If the address fails the screen, the request is rejected at the contract level and the address is added to the cached blocklist for subsequent interactions.

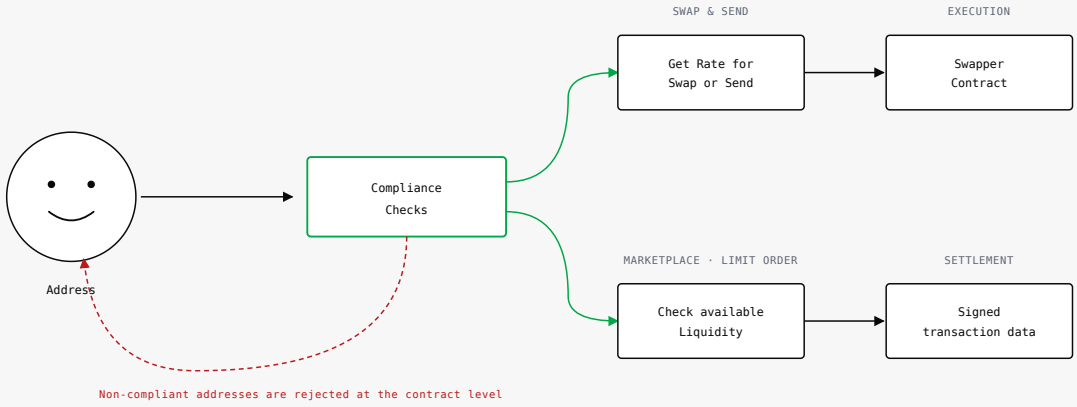

FIGURE 3.1 — COMPLIANCE GATE PROCESS FLOW, CONTRACT-LAYER ENFORCEMENT

Where the gate lives, technically

The compliance gate is implemented in two layers, designed to be redundant rather than alternative. Both layers must clear the same address against the same blocklist. Bypassing one layer does not result in access through the other.

LAYER	COMPONENTS	WHAT IT DOES
Application layer	`Front end · Public API · Relayer`	Refuses connection, quote, and order requests from blocklisted addresses. Handles the bulk of denials by avoiding wasted on-chain interactions.
Contract layer	`Swap router · Intent settlement · Marketplace`	Refuses execution from blocklisted addresses even if the application layer is bypassed. The blocklist is consulted at the contract entry point before any state-changing operation.

Blocklist update flow

The blocklist is maintained from the analytics providers' continuously-updated feeds. New OFAC designations, freshly attributed clusters, and risk-score upgrades propagate to the gate without operator intervention. The Sera operations team does not curate the blocklist manually; the team's role is to maintain the integration, monitor for provider availability, and review flagged false-positives raised through the disputes process described in Section 10.

Failure modes and conservative defaults

The gate fails closed by design. If the screening provider is unreachable at the time of a quote request, the gate denies the request and surfaces a transient error rather than allowing the request to proceed unchecked. This conservative default is consistent with the practice of regulated VASPs that integrate the same providers, and is preferred by Sera's compliance posture even though the protocol is not regulated.

Provider redundancy

Sera screens against more than one on-chain analytics provider. The use of multiple providers reduces single-source dependency, broadens typology coverage, and provides a cross-check on attribution edge cases. The specific providers in use are communicated to qualified counterparties on request, under separate confidentiality cover.

What is not screened at the protocol layer

Sera does not perform substantive Know Your Customer (KYC) on counterparties. Identity verification, source-of-funds documentation, and customer due diligence are the responsibility of the counterparty under their own AML programme. The protocol's screening operates on wallet-address attribution and transaction-pattern signals — not on identity documentation.

§ 04 · KNOW YOUR TRANSACTION (KYT)

Know Your Transaction *framework.*

KYT is the real-time monitoring layer. Every transaction routing through Sera is evaluated against high-risk typologies the moment it interacts with the protocol, with alerts surfacing within seconds and severity tiers driving automated action at the contract layer.

What KYT evaluates

KYT runs on every interaction — connection attempt, quote request, order placement, and swap execution. For each interaction, the screening engine evaluates the counterparty wallet against the live typology database, checks for direct exposure to known illicit clusters, and traces indirect exposure across multiple hops until an attributed service is reached. The result is a severity tier (low, medium, high, severe) plus a category-specific exposure profile.

Severity tiers and automated action

SEVERITY	TRIGGER	AUTOMATED ACTION
Severe	Direct exposure to OFAC SDN, comprehensively sanctioned jurisdiction, CSAM, or terrorism financing	Immediate, permanent denial. Address added to blocklist. No human review required to deny; manual review only required to remove.
High	Direct exposure to attributed mixers, hacks, ransomware, or darknet markets above threshold	Denial. Address added to blocklist. Eligible for case-by-case review on dispute.
Medium	Material indirect exposure to high-risk categories within tracing window	Denial subject to threshold settings. Reviewed periodically as attribution evolves.
Low	No material direct or indirect exposure	Permitted. Continuous re-evaluation on each interaction.

Continuous monitoring

KYT does not operate only at onboarding. The continuous-monitoring component re-evaluates wallet exposure on every subsequent interaction and propagates changes in risk score to the gate within seconds. A wallet that cleared the screen yesterday is screened again today; a wallet whose counterparty has since been attributed to a sanctioned cluster will be denied at next interaction without manual intervention.

Alert handling and case management

Severe and high-tier alerts are recorded in the compliance case management system with timestamps, severity, category, and the underlying analytics evidence. Records are retained for a minimum of seven years from the date of alert, in line with standard AML-record-retention practice, and are available for production to law enforcement on valid legal request.

What KYT does not do

KYT operates on on-chain data and analytics-provider attribution. It does not perform identity verification, sanctions screening of natural-person names, PEP screening, or adverse-media screening. These KYC functions are the responsibility of the counterparty under its own programme.

§ 05 · KNOW YOUR ADDRESS (KYA)

Know Your Address *framework.*

KYA is the wallet-level risk-scoring layer. It complements KYT by evaluating an address's full on-chain history and entity attribution before it is allowed to interact with the protocol — not just the present transaction, but the address's accumulated exposure profile.

What KYA evaluates

For every connecting address, KYA produces a risk profile that includes: (i) direct exposure to attributed entities in each typology category; (ii) indirect exposure across multiple hops, traced until an attributed service is reached; (iii) the address's interaction history with high-risk exchanges, mixers, and other risk-elevating services; and (iv) a composite risk score derived from the analytics provider's clustering and attribution methodology.

Direct vs indirect exposure

Direct exposure means the address has transacted directly with an attributed wallet — for example, sending to or receiving from a sanctioned address. Indirect exposure means the address has transacted with a wallet that itself transacted with an attributed wallet, possibly through several intermediate hops. Sera's KYA implementation evaluates both, going as many hops back as needed until an identified service or cluster is reached.

Indirect exposure is a deliberate design choice. Funds laundered through unhosted intermediary wallets — a common evasion technique — produce no direct exposure to the attributed source, but the chain of transactions remains traceable. Indirect-exposure tracing detects the laundering pattern that direct-exposure-only screening would miss.

Continuous score updates

Risk scores are not static. The analytics provider's attribution database expands continuously as new clusters are surfaced, new entities are attributed, and existing attributions are refined. An address's KYA score reflects the most recent attribution data at the time of evaluation, and is recomputed on every interaction.

Whitelist asymmetry

KYA produces a denial decision for addresses that exceed configured risk thresholds. It does not produce an affirmative whitelist — clearing the gate does not constitute a positive endorsement of the counterparty by Sera or by the analytics provider. Counterparties remain responsible for their own counterparty due diligence, of which KYA is one signal.

Tracing window

Indirect-exposure tracing is bounded by a tracing window — the maximum number of hops back from the connecting address that the analytics layer evaluates. Sera's tracing window is configured at industry-standard depth, calibrated to balance false-positive rates against laundering-pattern detection. The specific configuration is communicated to qualified counterparties on request.

KYT VS KYA — AT A GLANCE

KYT answers: *is this transaction, right now, exposed to a high-risk typology?* It runs on every interaction and produces a severity tier in real time.

KYA answers: *does this address, across its full history, present unacceptable counterparty risk?* It runs on every interaction and produces a composite risk profile.

The two frameworks are complementary. A wallet may pass KYT (this transaction is clean) but fail KYA (the wallet's history shows exposure that warrants denial), or vice versa. Sera enforces the stricter outcome.

§ 06 · TYPOLOGY COVERAGE

Typology coverage.

Eight categories of activity are explicitly covered by Sera's screening framework. Categories one through six are denied based on direct and material indirect exposure thresholds. Category seven is treated as zero-tolerance with no threshold. Category eight reflects upstream counterparty quality.

Category 01 — Sanctions exposure

Multi-list, multi-jurisdiction sanctions coverage including: U.S. Treasury Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list; the European Union's consolidated sanctions list; United Nations Security Council sanctions; the United Kingdom HMT consolidated list; addresses linked to comprehensively sanctioned jurisdictions including Russia, Iran, the Democratic People's Republic of Korea, Cuba, and Syria; and OFAC fifty-percent-rule beneficial-ownership clusters surfaced by the analytics provider.

Category 02 — Mixers and tumbling services

Custodial and non-custodial mixing services, privacy pools used for illicit-flow obfuscation, chain-hopping bridges used as obfuscation primitives, and any service whose attributed primary purpose is to break the on-chain trail between source and destination. This category includes both currently-active services and historical services whose addresses remain in the analytics database.

Category 03 — Hack, exploit, and ransomware proceeds

Wallets receiving funds traceable to public exchange hacks, bridge exploits, smart-contract drains, ransomware payouts, and the broader ransomware-affiliate ecosystem. Coverage includes both the proceeds wallets themselves and downstream wallets within the analytics provider's tracing window. New attributions propagate as forensic investigations progress.

Category 04 — Darknet markets

Vendor wallets, market administrator wallets, cash-out clusters associated with active or recently-shuttered darknet markets, and wallets with material indirect exposure to those markets across all major chains. The category covers both narcotics-focused markets and broader illicit-goods marketplaces.

Category 05 — Fraud, scams, and phishing

Rug-pull project wallets, romance-scam clusters, investment-scam payouts (including pig-butchering operations), phishing drainers, fraud-shop wallets, and addresses attributed to organised scam networks by the analytics provider. Both direct exposure and indirect exposure are scored, reflecting the prevalence of layering in scam-proceeds laundering.

Category 06 — Terrorism financing

Wallets attributed to designated terrorist organisations, fundraising wallets associated with violent-extremism actors, and clusters surfaced by the analytics provider's terrorism-financing typology. Coverage includes both organisations on national designation lists and organisations attributed by the provider's intelligence team where on-chain evidence supports attribution.

Category 07 — Child sexual abuse material (CSAM)

Wallets attributed to CSAM vendors and distribution clusters. This category is treated as **zero-tolerance**. Any direct or material indirect exposure results in immediate, permanent denial of access. There is no threshold; there is no review process for re-instatement at the protocol level. Where evidence supports referral, Sera will cooperate with law enforcement on valid legal request.

Category 08 — High-risk exchanges and unregistered VASPs

Exchanges with lax or absent KYC programmes, exchanges domiciled in FATF-deficient jurisdictions, and unregistered virtual-asset service providers with material exposure to the categories above. This category reflects upstream counterparty quality: a wallet with significant exposure to a no-KYC exchange is treated as carrying elevated counterparty risk, even if the wallet itself shows no direct exposure to attributed illicit sources.

Threshold configuration

Categories one through six are evaluated against severity thresholds. Direct exposure above the configured threshold results in denial; indirect exposure above the configured threshold results in denial. Threshold settings are calibrated against industry practice and reviewed quarterly. The specific threshold configuration is shared with qualified counterparties under separate confidentiality cover.

§ 07 · ACCESS RESTRICTIONS

Access restrictions.

Restrictions apply at both the application layer (front end and API) and the contract layer (swap router, intent settlement, marketplace). Funds custody is treated separately — see Section 08.

What a blocklisted address can and cannot do

CAPABILITY	COMPLIANT ADDRESS	BLOCKLISTED ADDRESS
Connect to Sera front end	✓ permitted	✗ refused at app layer
Receive a binding swap quote	✓ permitted	✗ refused at app layer
Place or cancel limit orders via API	✓ permitted	✗ refused at app layer
Execute swaps via swapper contract	✓ permitted	✗ refused at contract layer
Settle intents via intent contract	✓ permitted	✗ refused at contract layer
Read account data and trade history via API	✓ permitted	✗ refused at app layer
Withdraw owned tokens from the Vault	✓ permitted	✓ via emergencyWithdraw()

Application layer enforcement

Most denials are handled at the application layer. The front end refuses to connect blocklisted wallets, the public API refuses to accept requests, and the relayer refuses to assemble or broadcast intent transactions. This layer absorbs the bulk of denial traffic and prevents wasted on-chain interactions.

Contract layer enforcement

The contract layer is enforcement of last resort, designed to deny access even if the application layer is bypassed. The blocklist is consulted at contract entry points before any state-changing operation. An address that crafts and broadcasts a transaction directly — bypassing the front end and API — will still be refused at the contract entry point.

Why custody is separate

Note that the final row of the table above shows that a blocklisted address retains the ability to withdraw its own tokens from the Vault. This is intentional and architectural, not a gap in enforcement. The non-custodial design of the protocol means that user funds are never under Sera's control to seize, freeze, or redirect. The compliance gate restricts access to *services*; it does not, and architecturally cannot, restrict a depositor's access to their own *tokens*. This is the subject of Section 08.

§ 08 · NON-CUSTODIAL GUARANTEES

Non-custodial guarantees.

Sera is a non-custodial protocol. Wallet screening governs access to the protocol's services and routing. It does not — and architecturally cannot — affect a depositor's ability to retrieve tokens already held in the Vault contract.

The three properties

The non-custodial design rests on three properties of the Vault contract. Each property is verifiable on-chain, independently auditable, and confirmed in the CertiK audit referenced in Section 11.

01 **Property 01 — Ownership**

Vault balances are credited to the depositor's address. The contract does not contain any function that allows Sera, an administrator, a multisig, or an oracle to reassign a balance from one address to another. Vault balances are owned by the depositor and only by the depositor.

02 **Property 02 — Permissionless exit**

The Vault contract exposes an `emergencyWithdraw()` function that is callable directly by any depositor against their own balance. This function does not check the blocklist; it does not require the application layer; it does not require the API; it does not require Sera's involvement in any form. A depositor whose address is blocklisted retains full ability to withdraw their tokens by calling this function directly on-chain.

03 **Property 03 — No freeze primitive**

The Vault contract does not contain any function that allows funds to be frozen, seized, redirected, or rendered inaccessible. There is no admin key, no pause function applicable to user balances, no oracle signal that can disable withdrawal. The absence of a freeze primitive is verified by reading the contract source and confirmed in the audit.

What this means for the compliance posture

The compliance gate denies a blocklisted address access to Sera's services: the ability to obtain a quote, route a swap, place an order, or read account data. The gate does not — and cannot — interfere with the depositor's underlying property right in the tokens held in the Vault. The distinction is clear and architecturally enforced: **Sera can deny access to its services; Sera cannot touch user funds.**

Why this matters for institutional counterparties

For institutional liquidity providers, the non-custodial design means: (i) Sera does not pose custodial counterparty risk for deposited liquidity; (ii) regulatory action against Sera, if any were to occur, cannot result in seizure of LP-deposited tokens; (iii) the LP's right to withdraw is a property of the smart contract, not a contractual undertaking by Sera. This is materially different from the custodial-counterparty risk profile of a centralised exchange or a custodian.

Verification

The contract addresses listed in Section 11 are verified on Etherscan and may be inspected directly. The CertiK audit report, which confirms the absence of freeze primitives and the correctness of `emergencyWithdraw()`, is available to qualified counterparties on request.

§ 09 · COUNTERPARTY ASSURANCES FOR LPS

Counterparty assurances *for institutional LPs.*

When you provide liquidity on Sera, you quote against flow originating from screened addresses. The six controls below are designed to give institutional LPs and their compliance officers a defensible posture on counterparty risk, independent of Sera's own license status.

Control 01 — Counterparty pre-screening

Every taker that consumes your liquidity has cleared the same KYT and KYA screen described in Sections 04 and 05. You are not quoting into anonymous traffic. You are quoting into traffic that has passed a sanctions and high-risk filter at the contract layer. The same screening that protects Sera protects your fills.

Control 02 — Source-of-funds expectation

Liquidity providers are expected to deposit liquidity from wallets whose source of funds they can document under their own AML programme. Sera applies the same screening to LP addresses as to taker addresses, but does not perform substantive KYC on either side. Documentation of the LP's source of funds remains the LP's responsibility under their own programme.

Control 03 — On-chain audit trail

Every fill, every fee, every routing hop is recorded on-chain and independently verifiable. LPs and their auditors can reconstruct any time window directly from the chain — block by block, transaction by transaction — with no reliance on Sera-controlled databases. This is materially stronger than the audit-trail position of a counterparty whose records are held in a private database, because the on-chain trail is independently retained whether Sera is operational or not.

Control 04 — Sanctions list refresh

The blocklist is refreshed continuously against the analytics providers' feeds. New OFAC designations and freshly-attributed illicit-flow clusters propagate to the contract gate without operator intervention. The LP's compliance posture benefits from this propagation without any action required by the LP.

Control 05 — Indirect exposure tracing

Screening evaluates not only direct exposure but indirect exposure across multiple hops, until an attributed service is reached. This is significant for the LP's posture because funds laundered through unhosted intermediary wallets — a common evasion technique — produce no direct exposure to the attributed source. Indirect-exposure tracing detects the laundering pattern that a direct-exposure-only filter would miss.

Control 06 — Issuer eligibility upstream

Stablecoins routable on Sera are restricted to regulated, fully-reserved issuers. Algorithmic and crypto-collateralised stablecoins are not eligible for listing on the protocol. The eligibility criteria are:

ELIGIBLE	NOT ELIGIBLE
1:1 fiat-backed stablecoins (USD, EUR, SGD, etc.)	Algorithmic stablecoins
1:1 government-bond-backed stablecoins	Crypto-collateralised stablecoins
Regulated issuer entity	Commodity- or equity-backed tokens
Third-party attested reserves	Unregistered or unregulated issuers

Restricting listings to high-quality, fully-reserved stablecoins ensures that downstream integrators — payment providers, remittance networks, wallets — can route confidently through the network, and that liquidity providers are not quoting against assets carrying material reserve, depeg, or regulatory tail risks.

What LPs are not asked to do

Sera does not require LPs to perform KYC on takers, to retain transaction records on Sera's behalf, or to file regulatory reports on Sera's behalf. The compliance gate operates upstream of LP liquidity; the LP's responsibility extends to its own programme, not to Sera's compliance function.

Operational due diligence on Sera

Qualified institutional counterparties undertaking operational due diligence on Sera as a counterparty may request the following materials, which are released under non-disclosure cover where applicable:

01 **CertiK smart-contract audit reports**
Full surface coverage. Available now on request.

02 **Differential audit reports per protocol upgrade**
In development. Will be released as upgrades are completed.

03 **Monitoring and on-call runbook**
In development. Targeted release through 2026.

04 **Incident response procedures**
In development. Targeted release through 2026.

05 **Screening provider methodology summary**
Available on request under separate confidentiality cover.

06 **LP-side reporting endpoints**
In development. API endpoints for self-serve reporting.

Contact pathways for these materials are described in Section 10.

§ 10 · DISPUTES AND REMEDIATION

Disputes *and remediation.*

Address attribution is imperfect. The disputes process exists to surface false-positive classifications, channel them to the compliance review queue, and remove blocks where the underlying analytics evidence does not support them.

What constitutes a false positive

A false-positive classification is one in which the wallet has been blocked but the underlying analytics evidence does not support a denial under Sera's threshold configuration. False positives can arise from: incorrect entity attribution by the analytics provider; out-of-date attributions that have since been corrected; clustering errors that group an unrelated wallet with an attributed cluster; or misapplied thresholds in the gate's configuration.

How to submit a review request

Affected wallet holders, or counterparties acting on their behalf, may submit a review request through the compliance contact form hosted at `https://sera.cx/compliance`. Requests should include: the affected wallet address, the blockchain on which it operates, a brief description of the wallet's purpose, and any supporting evidence the holder considers relevant (transaction hashes, source-of-funds documentation, counterparty correspondence).

Review process and timelines

Review requests are queued in the compliance case management system. Initial acknowledgement is provided within one business day. Substantive review — including independent re-evaluation of the analytics evidence and, where appropriate, escalation to the analytics provider's investigation team — is targeted to complete within five business days for standard cases.

Cases involving severe-tier attributions (sanctions, terrorism financing, CSAM) are subject to enhanced scrutiny and may take longer; cases involving complex multi-hop attribution may take longer still.

Outcomes

01 **Block removed**

The classification is determined to be a false positive. The wallet is removed from Sera's local blocklist. The provider's underlying attribution may persist; the analytics provider has its own dispute process for upstream correction.

02 **Block upheld**

The classification is determined to be supported by evidence. The wallet remains on the blocklist. The reasons for upholding are communicated to the requestor at a level of detail consistent with the operational security of the screening framework.

03 **Escalation**

The case requires further investigation, additional evidence, or input from the analytics provider's team. Timelines are extended and the requestor is kept informed.

Permanent denial categories

Category 07 (CSAM) is treated as zero-tolerance with no review path at the protocol level. Other severe-tier attributions are reviewable but subject to enhanced scrutiny.

Funds access during dispute

The non-custodial guarantees described in Section 08 apply throughout the dispute process. A wallet whose access is restricted retains the ability to call `emergencyWithdraw()` against its own Vault balance regardless of dispute status. The dispute relates to access to Sera's services, not to the holder's property right in deposited tokens.

§ 11 · REFERENCES AND CONTRACT ADDRESSES

References *and contract addresses.*

The on-chain identifiers, audits, and reference materials referenced throughout this document. All contract addresses are deployed on Ethereum mainnet and are publicly verifiable on Etherscan.

Sera Protocol contract addresses (Ethereum mainnet)

COMPONENT	ADDRESS
Sera Vault	0xabf1f322c6626f283895597be3b8d52fc618ec21
Sera (main)	0xf25bf48392e9e402ef2661bf7530d0420716b565
Smart Order Router (SOR)	0x5a999e11a6959dbaafab93d2f64cd82497891681
Batcher	0x238399910636f41f351d20411ffae4deb8f2b9a5

Counterparties are encouraged to verify contract addresses against the canonical list published at `sera.cx/docs` before relying on them for due-diligence purposes.

Audits and security

Smart-contract audit firm	CertiK — full surface coverage with continuous monitoring
Audit scope	All contracts listed above, including Vault, main protocol, SOR, and Batcher
Audit reports	Available to qualified institutional counterparties on request

Compliance framework references

The compliance framework described in this document draws on the following external standards and frameworks. Sera is not bound to any of these as a regulated entity, but the framework is informed by them as a matter of voluntary best practice.

01 **FATF Recommendations**

In particular Recommendations 10–12 (CDD), 16 (wire transfers), and 20 (suspicious transaction reporting) — informing the KYT/KYA framework structure.

02 **OFAC sanctions guidance**

U.S. Department of the Treasury Office of Foreign Assets Control sanctions lists and 50%-rule guidance — informing the sanctions-exposure category.

03 **EU consolidated sanctions list, UN Security Council sanctions, UK HMT consolidated list**

Multi-jurisdiction sanctions coverage beyond the U.S.

Document contact

Contact regarding this document, requests for materials referenced herein, or compliance enquiries are channelled through the form at `https://sera.cx/compliance`. Direct email channels are not exposed publicly to reduce phishing and impersonation risk; the form routes to the appropriate compliance, legal, security, or institutional onboarding contact based on the enquiry type selected.

SERA COMPLIANCE FRAMEWORK · V1.0 · END

Compliant *by design.* Custody-free *by construction.*

For enquiries, false-positive review, institutional onboarding, regulator information requests, or operational due diligence pack requests, please use the form hosted at sera.cx/compliance.

DOCUMENT VERSION	ISSUED	PAGES
1.0	28 April 2026	23