BALDIVICIO & CO.

SOC 2 Trust Services Criteria

Document Title
Baldivicio SOC 2 Trust Services Criteria Compliance Paper

Document Type
Standards-oriented trust-services and control-governance narrative

Subject
Security, availability, processing integrity, confidentiality, and privacy governance within Baldivicio

Effective Date
April 13, 2026

1. Introduction

This paper explains Baldivicio's control posture through the lens of SOC 2 and the Trust Services Criteria. It is intended to provide a comprehensive and structured account of how Baldivicio's service model, custodial framework, onboarding controls, transaction controls, privacy practices, incident-response measures, continuity safeguards, and account-governance processes support a trust-oriented operating environment for a digital financial service.

Baldivicio is a digital financial services platform made available primarily through its mobile application. Across its service, privacy, operational, and legal materials, Baldivicio states that it currently supports USDC-only activity on Ethereum Mainnet through a custodial model, that Baldivicio holds and manages the private keys associated with supported wallet functionality on behalf of users, and that users do not receive, possess, or export private keys. The service is also described as operating in a security-sensitive, compliance-sensitive, privacy-sensitive, and blockchain-connected environment in which identity verification, account protection, transaction review, service continuity, and legal controls are important parts of everyday operations.

SOC 2 is concerned with whether a service organization has established controls that support trust in how the service is operated. In Baldivicio's context, that means attention to the secure administration of accounts, protection of users and their information, resilience of service delivery, integrity of transaction-related workflows, bounded disclosure of information, and the ability to intervene when misuse, fraud, suspicious activity, technical disruption, or other risk conditions arise.

This paper is written as a governance and compliance document. It is not a product brochure, not a customer marketing statement, and not a substitute for detailed engineering or internal operational documentation. Its purpose is to explain, in standards-oriented language, how Baldivicio's service framework aligns with the major themes of the Trust Services Criteria while remaining faithful to the control boundaries and service claims expressed across Baldivicio's published materials.

2. Purpose and Objectives

The purpose of this paper is to document how Baldivicio's operating framework can be understood in relation to the Trust Services Criteria commonly associated with SOC 2.

The Trust Services Criteria focus on whether an organization's systems and controls support the objectives of Security, Availability, Processing Integrity, Confidentiality, and Privacy. For Baldivicio, these themes are highly relevant because the platform processes sensitive identity and account information, supports custodial digital-asset functionality, handles transaction instructions, delivers legally significant electronic communications, relies on third-party services in certain connected workflows, and must maintain service integrity in the face of fraud, suspicious activity, outages, degraded conditions, and legal obligations.

The objectives of this paper are fivefold.

First, it explains the service environment in which Baldivicio's trust-services obligations arise.

Second, it establishes the control themes that recur across Baldivicio's policies, disclosures, and service descriptions.

Third, it explains how those controls relate to the SOC 2 Trust Services Criteria.

Fourth, it presents a structured narrative suitable for governance, legal, operational, compliance, privacy, security, and risk review.

Fifth, it defines the scope and boundaries of the narrative without making technical, procedural, or assurance claims beyond what Baldivicio's public service framework supports.

3. Scope

This paper applies to Baldivicio's digital service environment to the extent that environment bears on trust, control, service integrity, and information governance.

It therefore addresses the Trust Services Criteria as reflected in:

- the mobile application and related digital service channels;
- website interactions where relevant;
- account onboarding, identity verification, and eligibility review;
- custodial wallet functionality and supported USDC activity on Ethereum Mainnet;
- access control, credential handling, device and session awareness, and suspicious-access review;
- transaction handling, transaction review, transaction restrictions, and transaction execution workflows;
- customer support, dispute handling, and electronic communications;
- privacy and personal-information handling;
- monitoring, logging, audit trails, record retention, and evidentiary preservation;
- incident handling, outage and degradation response, emergency maintenance, and reconciliation;
- account restriction, suspension, freezing, and closure processes; and
- third-party-connected workflows, including those involving Banxa and other service providers where applicable.

This paper should be read consistently with Baldivicio's Terms of Service, Privacy Policy, Acceptable Use Policy, Deposit Insurance Disclosure, Reserve and Transparency Attestation, Customer Identification Program Notice, E-Sign Consent and Electronic Communications Agreement, Fee Schedule and Schedule of Charges, Irreversible Transactions Disclosure, System Outage and Degradation Policy, and Account Suspension, Freezing, and Closure Policy.

4. Service Context Relevant to the Trust Services Criteria

Baldivicio's trust posture must be understood in relation to the service it provides. Baldivicio is a digital financial services platform delivered primarily through a mobile application rather than through branch-based or paper-based channels. Its service model combines digital onboarding, identity verification, custodial wallet functionality, account and transaction review, customer support, compliance controls, and electronic communications.

This means the Trust Services Criteria apply not to a single isolated software component, but to a broader operational environment in which service reliability, information protection, lawful access, transaction accuracy, user communication, fraud prevention, and service-continuity measures all contribute to trustworthiness.

The platform also expressly recognizes dependencies on internet connectivity, cloud and supporting infrastructure, email and notification channels, blockchain network conditions, and third-party providers involved in connected service workflows. These dependencies matter because SOC 2-oriented trust is not measured solely by direct application features. It is also shaped by operational boundaries, response capabilities, and the organization's ability to manage reliance on supporting systems and external service participants.

5. Foundational Trust Position

Baldivicio's foundational trust position is that the service is operated through layered, risk-aware, and intervention-capable controls that support secure and reliable delivery of custodial digital financial services.

This position is visible throughout the service framework. Baldivicio describes its platform as built around security, compliance, and usability. It refers to protected sign-in flows, secure credential handling, device-level trust signals, continuous checks supporting verification of account activity, structured onboarding and review, controlled transaction workflows, account-lifecycle governance, privacy and

information-handling safeguards, outage and degraded-service response, and the ability to restrict or suspend activity when service integrity, legal compliance, or customer protection require it.

In SOC 2 terms, these features show that trust is treated as an operational outcome supported by documented controls rather than by a narrow promise of uptime or a single technical safeguard. Security, availability, processing integrity, confidentiality, and privacy are all reflected in the way the service is structured and governed.

6. Common Control Environment Themes

Before addressing the individual Trust Services Criteria, it is useful to identify the common control themes that appear across Baldivicio's framework.

The first theme is governed digital service delivery. Baldivicio delivers financial functionality through a controlled service environment rather than through unmanaged customer-side infrastructure.

The second theme is account-state control. Access to functionality depends on onboarding completion, identity verification, legal eligibility, security review, fraud review, compliance status, and operational conditions.

The third theme is layered review. Sensitive actions may be subject to validation, delay, restriction, refusal, enhanced review, or manual review where circumstances require it.

The fourth theme is evidentiary traceability. Account events, transaction records, access records, communications, compliance materials, incident records, and support interactions are treated as relevant records within the operating environment.

The fifth theme is controlled intervention. Baldivicio may restrict, suspend, freeze, close, or otherwise limit activity to protect users, comply with law, preserve service integrity, or respond to suspicious or abnormal conditions.

The sixth theme is continuity-aware operation. Planned maintenance, emergency maintenance, degradation, external dependency failure, and post-incident reconciliation are expressly recognized parts of the service model.

The seventh theme is privacy-aware service delivery. Personal information handling is described through a structured privacy framework that addresses collection, use, sharing, retention, rights, public-blockchain limitations, and third-party processing relationships.

These common themes provide the basis for a Trust Services Criteria analysis.

7. Security Criterion

The Security criterion is concerned with whether the system is protected against unauthorized access, unauthorized disclosure, misuse, or damage in ways that could compromise the service or its users. Baldivicio's service framework strongly supports this criterion.

Security is built into the Baldivicio service model from onboarding through ongoing account use. The platform refers to protected sign-in flows, secure credential handling, device-level trust signals, continuous checks that help verify account activity, authentication measures, monitoring, account-protection notices, and the ability to analyze technical and behavioral information to detect suspicious access, account takeover risk, fraud, misuse, or evasion of compliance and security controls.

The service also links access to account status and review state rather than treating access as a purely static entitlement. Identity verification may be required before or during use of the service. Incomplete or unsatisfactory onboarding, suspicious activity, device compromise, compliance concerns, legal restrictions, or fraud-related concerns may lead to delayed access, enhanced review, limitation of functionality, suspension, freezing, or closure.

The custodial model is also important to the Security criterion. Baldivicio states that it holds and manages the private keys associated with supported wallet functionality and that users do not export those keys. This concentrates responsibility for critical wallet control within Baldivicio's service boundary and reduces direct user-side exposure of sensitive key material.

The Acceptable Use Policy further strengthens the Security criterion by prohibiting attempts to probe, disrupt, bypass, or compromise Baldivicio's systems or controls, as well as phishing, impersonation, cybercrime-related misuse, malware-related activity, credential theft, and other abusive conduct. These prohibitions are reinforced by enforcement powers that allow Baldivicio to intervene when service integrity is threatened.

Together, these features support a strong narrative that Baldivicio's service is designed to protect against unauthorized access, misuse, and abusive activity through layered security, monitoring, identity assurance, and intervention measures.

8. Availability Criterion

The Availability criterion addresses whether the system is available for operation and use as committed or agreed. Baldivicio's service framework approaches availability in a disciplined and realistic way.

Baldivicio does not promise uninterrupted or error-free service. Instead, it acknowledges the possibility of outages, degraded performance, maintenance events, software defects, infrastructure failures, blockchain disruptions, third-party provider failures, communications issues, legal restrictions, and operational anomalies. This is important because it frames availability as a managed operational objective rather than an absolute guarantee.

The System Outage and Degradation Policy explains that Baldivicio may perform planned maintenance, emergency maintenance, upgrades, remediation, rollback, recovery measures, and post-incident reconciliation. It also explains that Baldivicio may monitor and diagnose issues, isolate affected components or workflows, temporarily disable or limit features, delay transaction execution, restrict account actions, coordinate with cloud and infrastructure providers, and later restore or reconcile state.

The service materials further recognize that availability of functionality may depend on internal systems, blockchain network conditions, internet and cloud infrastructure, email or notification channels, fraud and compliance controls, and third-party provider systems. This means availability is treated as a service-wide operational concern involving both direct and external dependencies.

From a SOC 2 perspective, this reflects a mature availability posture. Availability is supported by explicit recognition of operational risk, structured handling of outages and degraded conditions, emergency intervention capability, communications processes, and reconciliation after restoration.

9. Processing Integrity Criterion

The Processing Integrity criterion is concerned with whether system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives. This is one of the most important trust criteria for Baldivicio because the service involves digital financial activity and custodial transaction processing.

Baldivicio's service framework repeatedly emphasizes that financial activity is handled through controlled workflows designed to prioritize accuracy, authorization, and traceability. Users submit instructions through the service rather than exercising unmanaged direct signing authority. Baldivicio may validate requests, review destinations, apply risk checks, delay or refuse transactions, impose destination restrictions, monitor pending and completed transfers, and enforce account-state, fraud, compliance, and operational controls before execution.

The Irreversible Transactions Disclosure reinforces the importance of processing integrity by making clear that not every submitted instruction becomes final immediately and that Baldivicio may apply review, delay,

restriction, or refusal before execution. Once execution occurs, however, transactions may become irreversible. This means integrity controls must be strongest before execution, and Baldivicio's framework clearly recognizes that.

The platform also addresses duplicate-submission risk, delayed status-display risk, and the need for validation and reconciliation after outages or degraded conditions. The System Outage and Degradation Policy explains that repeated submissions during an incident may create duplication risk and that post-incident reconciliation may be necessary to confirm the status of transactions, balances, restrictions, or notifications.

Taken together, these elements strongly support the Processing Integrity criterion. The service does not present transaction handling as informal or purely user-driven. It is processed through authorization, review, monitoring, reconciliation, and operational state controls designed to support valid and properly governed outcomes.

10. Confidentiality Criterion

The Confidentiality criterion addresses whether information designated as confidential is protected in accordance with the entity's commitments and system requirements. Baldivicio's framework supports this criterion in several ways.

The custodial model itself implies strong confidentiality obligations. Baldivicio holds and manages the private keys associated with supported wallet functionality, and users do not export them. While the public service framework does not describe underlying implementation specifics, it makes clear that sensitive wallet-control material remains within Baldivicio's service boundary.

The Privacy Policy also describes protective measures that support confidentiality more broadly. These include access controls, authentication measures, environment segregation, monitoring, encryption or protected transmission where appropriate, audit logging, vendor controls, incident-response measures, and data minimization where reasonably practicable. The service framework also supports controlled disclosure by identifying categories of recipients and lawful or service-related circumstances in which information may be disclosed.

Support interactions, compliance materials, identity-verification records, transaction records, device and access records, and legal or investigative materials are all recognized as part of the sensitive information environment. The Privacy Policy and related documents make clear that such information is retained and used for defined operational, legal, security, and compliance purposes rather than disclosed freely or without governance.

It is also important that Baldivicio distinguishes between off-chain confidential information and information that may exist on public blockchain infrastructure. This helps define the boundaries of confidentiality realistically, which is itself an important aspect of trust.

11. Privacy Criterion

The Privacy criterion addresses the collection, use, retention, disclosure, and disposal of personal information in conformity with commitments and requirements. Baldivicio's Privacy Policy provides a substantial framework in support of this criterion.

Baldivicio explains what categories of personal information it may process, how information may be collected, the purposes for which it may be used, the categories of recipients with whom it may be shared, the role of third-party providers such as Banxa, the possibility of international transfers, the use of cookies or similar technologies where relevant, the retention model for personal information, the security measures applied to protect that information, the rights that users may have depending on applicable law, and the limits that may apply to those rights.

The Privacy Policy also recognizes the special privacy characteristics of blockchain-connected activity. It states that certain transaction-related information may exist on public blockchain infrastructure, may be visible to third parties, and may remain visible indefinitely. This transparency is especially important for a digital-asset service because it helps set realistic privacy expectations and distinguishes between off-chain personal-information protection and public-ledger visibility.

The policy further explains that personal information may continue to be processed and retained during account review, restriction, suspension, freezing, or closure where necessary for legal, compliance, security, dispute-resolution, evidentiary, or operational purposes. This is consistent with the realities of a financial service operating in a regulated environment.

From a SOC 2 perspective, these features support a strong Privacy criterion narrative. Baldivicio provides structured notice, purpose-linked processing, bounded disclosure, retention governance, user-rights recognition, and privacy-aware security safeguards.

12. Control Environment and Governance Structure

A core SOC 2 concern is whether the control environment is coherent and governed rather than ad hoc. Baldivicio's service framework strongly supports that perspective.

The platform is supported by a layered policy environment. The Terms of Service define the overall service relationship and user responsibilities. The Acceptable Use Policy defines permitted and prohibited conduct. The Customer Identification Program Notice governs identity-related data collection and review. The Privacy Policy governs personal-information handling and related security measures. The E-Sign Agreement governs electronic communications. The Irreversible Transactions Disclosure governs transaction-finality and pre-execution risk. The Outage and Degradation Policy governs abnormal service conditions and recovery processes. The Account Suspension, Freezing, and Closure Policy governs containment and lifecycle enforcement. The Reserve and Transparency Attestation and Deposit Insurance Disclosure define service and risk boundaries relevant to customer understanding and operational expectations.

Taken together, these documents create a control environment in which obligations, restrictions, service limitations, intervention powers, and information-handling rules are expressly described rather than implied. That is a significant feature of a trust-services-oriented control framework.

13. Risk Awareness and Service Integrity

Trust in a digital financial service depends on recognition of risk and the ability to respond to it. Baldivicio's framework reflects this consistently.

The service identifies risks relating to fraud, phishing, account takeover, inaccurate onboarding information, suspicious activity, sanctions concerns, security issues, blockchain congestion, outages, external provider failures, legal restrictions, and operational anomalies. Each of these risks is tied to practical control responses such as additional information requests, destination restrictions, review holds, suspension, freezing, closure, emergency maintenance, reconciliation, or post-incident validation.

This means service integrity is not assumed. It is maintained through active management of risk conditions. In SOC 2 terms, this supports the view that Baldivicio's trust posture is operationally grounded rather than aspirational.

14. Access Controls and User Authentication

Access controls are essential to both the Security and Confidentiality criteria. Baldivicio's framework provides strong support for them.

The service refers to protected sign-in flows, secure credential handling, device-level trust signals, authentication events, session records, account access history, suspicious-sign-in review, and technical and behavioral analysis intended to help detect suspicious access and account-compromise risk. Users are expressly responsible for safeguarding credentials and devices and for promptly reporting suspected unauthorized access or suspicious activity.

Access is also governed by more than authentication alone. Functionality may be limited based on account status, verification completion, fraud review, compliance review, legal eligibility, or service conditions. This creates a layered access-control model in which login, authorization, and eligibility are related but distinct control points.

15. Onboarding, Verification, and Trust Enforcement

Baldivicio's onboarding and verification processes also support the Trust Services Criteria. Identity verification is required to help protect users, maintain service integrity, and comply with legal obligations. The service may request identifying information, government-issued identification, compliance-related information, and additional materials where appropriate. Automated systems, manual review, and third-party support may be used to verify information and assess eligibility or risk.

This is relevant to SOC 2 because onboarding and verification are part of the control environment through which trusted account access is established. They help reduce the risk of fraudulent accounts, misrepresentation, unauthorized use, and misuse of sensitive service functions.

16. Transaction Controls and Customer Protection

Because Baldivicio provides supported digital-asset functionality, transaction controls are central to trust.

Users are responsible for reviewing transaction details carefully before submission, including destination details, supported asset and network, amount, and other relevant information. Baldivicio may review destinations, apply fraud or compliance checks, delay or refuse execution, and investigate disputes. Completed transactions may become irreversible, and users are expressly warned not to assume that completed blockchain-related transfers carry the same reversal or chargeback protections as conventional payment methods.

This framework supports trust by making transaction-control boundaries clear. It also supports processing integrity and customer understanding of the service's limitations.

17. Monitoring, Logging, and Audit-Relevant Evidence

SOC 2 places importance on whether controls are supported by traceability and evidence. Baldivicio's framework supports this substantially.

The Privacy Policy states that Baldivicio may process authentication events, session records, account access history, device and access signals, transaction instructions, source and destination addresses, transaction hashes, timestamps, blockchain confirmations, state changes, review status, execution timing, routing data, support interactions, escalation records, incident logs, audit trails, and legal or investigative materials. The outage and account-control policies also refer to monitoring, diagnosing, reconciliation, validation, preservation of records, and follow-up review.

This creates a strong trust-services narrative around evidentiary support. Operational events, access events, transaction state, review status, and incident conditions can be monitored and preserved rather than left opaque.

18. Incident Response and Service Containment

SOC 2 trust also depends on whether the organization can respond appropriately when things go wrong. Baldivicio's framework clearly supports this area.

During or after incidents, Baldivicio may monitor and diagnose issues, isolate affected components or workflows, temporarily disable or limit features, delay or suspend execution, restrict account actions, apply enhanced review measures, perform emergency maintenance, coordinate with infrastructure and third-party providers, preserve records, and carry out post-incident reconciliation. Where appropriate and legally permitted, users may receive incident-related or service-state communications through available channels.

The account-control framework adds another layer by allowing restriction, suspension, freezing, or closure where fraud, unauthorized access, suspicious activity, operational anomalies, or legal requirements make such action appropriate.

These response capabilities are highly relevant to the Security, Availability, and Processing Integrity criteria.

19. Recovery and Post-Incident Restoration

A trust-oriented service environment must also be capable of restoring operations in a controlled way after disruption. Baldivicio's framework provides for this.

The Outage and Degradation Policy explains that restoration may involve remediation, rollback, recovery measures, validation of transaction state, reconciliation of affected balances or transactions, correction of delayed status display, restoration of records or notifications, and follow-up review where necessary. Users may temporarily encounter delayed history updates, pending indicators, incomplete records, or other residual effects while reconciliation is underway.

This recovery model is important because it recognizes that trustworthy restoration requires more than restarting service infrastructure. It also requires restoring reliable state, records, and service integrity.

20. Third-Party Providers and Service Dependencies

The Trust Services Criteria also require attention to the role of third parties. Baldivicio's framework is explicit on this point.

Baldivicio may use service providers for cloud hosting, infrastructure support, email delivery, analytics, identity verification, sanctions screening, fraud detection, compliance support, record storage, customer support tooling, security monitoring, and incident management. Certain connected financial or operational services may involve Banxa or other third-party providers. Service disruptions may also originate in whole or in part from external providers, internet or telecommunications failures, push-notification systems, app distribution platforms, or blockchain infrastructure.

This means that trust in the Baldivicio service depends not only on direct application controls but also on recognition and governance of external dependencies. The service framework addresses this by clearly stating that some processing, timing, communications, settlement outcomes, and restoration timing may depend in part on third-party systems or decisions.

21. Confidential Communications and Electronic Delivery

The E-Sign Consent and Electronic Communications Agreement contributes significantly to Baldivicio's trust posture. It explains the categories of electronic communications covered by the service, the methods by which they may be delivered, the technical capabilities users need to access them, the option to request paper copies in some cases, the effects of withdrawing consent, and the possibility of delays or interruptions arising from maintenance, outages, legal restrictions, or third-party issues.

This is relevant to SOC 2 because service trust is supported not only by secure processing but also by predictable, governed delivery of notices, records, and legally significant communications.

22. Confidentiality and Public Blockchain Boundaries

A particularly important part of Baldivicio's trust posture is its treatment of confidentiality boundaries in a blockchain-connected service.

The service makes clear that off-chain records, identity information, device and access signals, support records, compliance materials, and other service data are subject to protective measures and bounded disclosure. At the same time, Baldivicio also makes clear that certain transaction-related data may exist on public blockchain infrastructure, may be visible to third parties, may be analyzed or correlated, and may remain visible indefinitely.

This distinction is important to trust because it prevents the service from overstating confidentiality in an environment where some transaction-related visibility is inherently public. A realistic and transparent account of these limits is itself an important control feature.

23. Account Restrictions, Suspension, Freezing, and Closure

The account-control framework also contributes materially to the Trust Services Criteria.

Baldivicio may restrict, suspend, freeze, review, or close accounts where necessary for security, fraud prevention, legal compliance, operational protection, account integrity, or customer safety. Restrictions may affect access to balances, outbound transfers, withdrawals, funding or payout functions, and account changes. User-requested closure may also require the wallet balance to be drained before closure can be completed.

This control structure supports security, availability, and processing integrity by giving Baldivicio a mechanism to contain risk and preserve service integrity when conditions make unrestricted use inappropriate.

24. Privacy Rights, Retention, and Post-Closure Handling

The Privacy criterion is further supported by Baldivicio's treatment of rights, retention, and post-closure handling.

Depending on applicable law, users may have rights to request access, correction, deletion, restriction, objection, portability, consent withdrawal, or the ability to lodge complaints. These rights are not absolute and may be limited where necessary to preserve legal obligations, fraud prevention, compliance screening, dispute handling, evidentiary preservation, or service integrity.

Records may be retained for service provision, legal obligations, compliance, dispute resolution, enforcement, fraud prevention, security, audits, and lawful inquiries. After account restriction or closure,

personal information may continue to be processed and retained where reasonably necessary for those purposes. Public blockchain records may remain visible after closure and cannot be removed by Baldivicio.

This reflects a mature trust posture in which privacy promises are balanced against operational, legal, and security realities.

25. Conformance-Oriented Reading of the Trust Services Criteria

Read against the Trust Services Criteria as a whole, Baldivicio's service framework supports a coherent control narrative.

Under Security, Baldivicio supports protected access, credential handling, device and session awareness, fraud detection, suspicious-activity review, custodial key control, and intervention authority.

Under Availability, Baldivicio supports planned maintenance, emergency maintenance, outage handling, degraded-service response, coordination with external providers, restoration measures, and post-incident reconciliation.

Under Processing Integrity, Baldivicio supports controlled transaction workflows, validation and review before execution, structured account states, transaction-state awareness, duplicate-submission awareness, and reconciliation after abnormal conditions.

Under Confidentiality, Baldivicio supports access controls, authentication measures, environment segregation, monitoring, audit logging, vendor controls, bounded disclosure practices, and a clearly defined custodial service boundary.

Under Privacy, Baldivicio supports structured notice, purpose-linked processing, bounded information sharing, third-party-processing transparency, retention governance, user-rights recognition, security protection for personal information, and clear acknowledgment of public-blockchain privacy limits.

Taken together, these themes support a standards-oriented view of Baldivicio as a service organization operating through layered controls that are meaningfully aligned with the logic of the SOC 2 Trust Services Criteria.

26. Boundaries of This Paper

This paper is intentionally limited to matters established by Baldivicio's published service descriptions, policies, disclosures, and operating framework.

It does not describe technical implementation details that are not stated in those materials. It does not specify internal committee structures, testing schedules, infrastructure topology, encryption architecture, change-management tooling, secure development lifecycle controls, privileged-access workflows, backup architecture, or other implementation-specific controls not expressly described in Baldivicio's service framework.

It also does not transform service disclosures into technical or assurance claims beyond what they support. Where Baldivicio's materials describe a control objective, service principle, or intervention authority at a high level, this paper states that matter at the same level and does not convert it into an unsupported implementation-specific assertion.

27. Conclusion

Baldivicio's service framework establishes a clear and disciplined trust-oriented operating posture for a digital financial-services environment. The platform is delivered digitally, depends on secure onboarding

and account access, supports custodial wallet functionality, processes sensitive identity and transaction-related information, relies on monitored and reviewable workflows, and maintains defined powers to intervene, restrict, reconcile, and restore service where necessary.

The resulting control environment is not limited to any one criterion in isolation. It is reinforced by layered access controls, privacy and confidentiality safeguards, transaction validation and review, service continuity measures, outage and degradation response, record retention and auditability, third-party dependency awareness, and account-lifecycle controls. Together, these elements create a coherent standards-oriented narrative in which trust is supported through documented governance, operational safeguards, and bounded service commitments.

Accordingly, Baldivicio's SOC 2 Trust Services Criteria posture is best characterized as a control-driven, risk-aware, service-integrated framework in which security, availability, processing integrity, confidentiality, and privacy are supported through layered policies, operational controls, monitoring, communications governance, and protective intervention capability.

28. Final Statement

This paper should be read as Baldivicio's SOC 2 Trust Services Criteria compliance narrative in the context of its digital financial-services model. It reflects the service architecture, control positions, operational safeguards, privacy practices, continuity measures, and governance principles expressed across Baldivicio's published policies, disclosures, and service descriptions, and it should be interpreted consistently with those materials.