# SOC 2 REPORT

*For*

*Fino Partners Group, Inc.*

# SOC 2 Report Fino Partners Group, Inc.

## Contents

# 1. Independent Service Auditor's Report

To the Management of **Fino Partners Group, Inc.** and Its User Entities

We have examined the accompanying description of **Fino Partners Group, Inc.'s** system applicable to the **Trust Services Criteria for Security, Confidentiality, Processing Integrity, and Availability** (the "system"), as well as the suitability of the design and operating effectiveness of the controls stated in the system description.

The system description and the suitability of the design of controls were examined **as of January 7, 2026**. The operating effectiveness of the controls was examined **for the period January 1, 2025 to December 31, 2025**.

Management of Fino Partners Group, Inc. is responsible for preparing the system description and for the design and operating effectiveness of the controls to achieve the service commitments and system requirements based on the applicable Trust Services Criteria. Our responsibility is to express an opinion on the fair presentation of the system description, the suitability of the design of the controls, and the operating effectiveness of the controls based on our examination.

We conducted our examination in accordance with **attestation standards established by the American Institute of Certified Public Accountants (AICPA)**. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the system description is fairly presented, the controls were suitably designed, and the controls operated effectively to achieve the applicable service commitments and system requirements.

An examination of a service organization's system description and controls includes performing procedures to obtain evidence about the fair presentation of the description and the suitability and operating effectiveness of the controls. The procedures selected depend on the service auditor's judgment, including the assessment of risks that the system description is not fairly presented or that the controls were not suitably designed or did not operate effectively.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinions.

**Opinion on the Fair Presentation of the System Description**

*(As of January 7, 2026 – SOC 2 Type 1 & Type 2)*

In our opinion, in all material respects, the accompanying system description fairly presents **Fino Partners Group, Inc.'s** system applicable to the **Trust Services Criteria for Security, Confidentiality, Processing Integrity, and Availability as of January 7, 2026**.

**Opinion on the Suitability of the Design of Controls**

*(As of January 7, 2026 – SOC 2 Type 1 & Type 2)*

In our opinion, in all material respects, the controls described in the system description were **suitably designed as of January 7, 2026**, to provide reasonable assurance that the applicable service commitments and system requirements would be achieved **if the controls operated effectively**.

**Opinion on the Operating Effectiveness of Controls**

*(For the period January 1, 2025 to December 31, 2025 – SOC 2 Type 2 Only)*

In our opinion, in all material respects, the controls described in the system description **operated effectively throughout the period from January 1, 2025 to December 31, 2025**, to provide reasonable assurance that the applicable service commitments and system requirements were achieved based on the **Trust Services Criteria**.

# 2. Management's Assertion

Management of **Fino Partners Group, Inc.** is responsible for the accompanying description of the Company's system applicable to the **Trust Services Criteria for Security, Confidentiality, Processing Integrity, and Availability** (the "system") and for the design and operating effectiveness of the controls to achieve the related service commitments and system requirements.

**Assertion Regarding the Fair Presentation of the System**

*(As of January 7, 2026 – SOC 2 Type 1 & Type 2)*

Management asserts that the accompanying system description **fairly presents, in all material respects**, Fino Partners Group, Inc.'s system applicable to the Trust Services Criteria **as of January 7, 2026**.

The criteria used in making this assertion were that the system description:

- Presents how the system was designed and implemented
- Includes the services covered and the boundaries of the system
- Describes the components of the system, including infrastructure, software, people, procedures, and data
- Identifies the applicable Trust Services Criteria and related controls

**Assertion Regarding the Suitability of the Design of Controls**

*(As of January 7, 2026 – SOC 2 Type 1 & Type 2)*

Management asserts that the controls described in the system description were **suitably designed as of January 7, 2026**, to provide reasonable assurance that the Company's service commitments and system requirements based on the applicable **Trust Services Criteria** would be achieved **if the controls operated effectively**.

## SOC 2 Report Fino Partners Group, Inc.

**Assertion Regarding the Operating Effectiveness of Controls**

*(For the period January 1, 2025 to December 31, 2025 – SOC 2 Type 2 Only)*

Management asserts that the controls described in the system description **operated effectively throughout the period from January 1, 2025 to December 31, 2025**, to provide reasonable assurance that the Company's service commitments and system requirements based on the applicable Trust Services Criteria were achieved.

# 3. Section III – System Description

**System Description of Fino Partners Group, Inc.**

*(Applicable to SOC 2 Type 1 and SOC 2 Type 2)*

## 3.1 Organization Overview

**Nature of Business**

Fino Partners Group, Inc. is a professional services organization providing outsourced accounting, bookkeeping, tax support, and financial operations services to U.S.-based businesses and accounting firms. Services are delivered remotely using secure information systems and controlled operating environments.

In the course of providing services, the organization processes and accesses confidential financial, tax, and business information that is subject to information security and data protection requirements.

**Services Provided**

Services provided include outsourced accounting services, bookkeeping services, tax preparation and tax support services, and financial operations support. These services rely on

secure access to client systems, secure data transmission, and controlled handling of sensitive information.

**Role as a Service Organization**

Fino Partners Group, Inc. operates as a **service organization** for purposes of SOC 2 reporting, as it provides services that involve the processing, storage, transmission, and protection of client data using information technology systems. The organization is responsible for controls related to security, confidentiality, processing integrity, and availability within the defined system boundaries.

## 3.2 System Overview

**Description of Services Covered by SOC 2**

The SOC 2 system includes the information technology systems, people, procedures, and data used to support secure service delivery. The system supports:

- Secure access to client accounting and financial systems
- Processing and handling of client financial and tax data
- Secure communication and document exchange
- Monitoring, logging, and incident response activities

**System Boundaries**

The system boundary includes company-managed endpoints, secure cloud platforms, internal systems, and controlled access to client systems used in service delivery. Client-owned systems and infrastructure are outside the system boundary, except where accessed by authorized personnel for service delivery.

The system description assumes that user entities have implemented applicable **Complementary User Entity Controls (CUECs)** related to their own environments.

## 3.3 Trust Services Criteria in Scope

The following **Trust Services Criteria (TSC)** are included in the SOC 2 scope:

**Security**

Controls are designed to protect systems and data against unauthorized access, disclosure, or damage through logical access controls, endpoint security, monitoring, and incident response procedures.

**Confidentiality**

Controls are designed to protect confidential client financial and tax information through restricted access, secure transmission, encryption practices, and confidentiality requirements.

**Processing Integrity**

Controls are designed to support accurate, complete, and timely processing of information used in service delivery, consistent with defined procedures and client instructions.

**Availability**

Controls are designed to support system reliability and operational continuity, including secure cloud platforms, monitoring activities, and incident management procedures.

## 3.4 System Components

### 3.4.1 Infrastructure

**Secure Network Environment**

The organization maintains a secure network environment to support remote service delivery. Network controls are designed to restrict unauthorized access and protect data transmitted between systems.

**Cloud Platforms**

Secure, cloud-based platforms are used to support operational activities, communication, and document management. These platforms are approved by management and configured to support security and availability requirements.

**Endpoint Devices**

Company-managed endpoint devices are used by personnel to access systems and client environments. Endpoint security controls include device hardening, antivirus protection, restricted administrative privileges, and automatic screen locking.

### 3.4.2 Software

**Internal Systems**

Internal systems are used to support operational workflows, secure communication, monitoring, and document management. Access to internal systems is restricted based on role and business need.

**Client Systems Accessed**

Authorized personnel access client accounting and financial systems solely for the purpose of providing contracted services. The organization does not host or administer client systems.

### 3.4.3 People

**Roles and Responsibilities**

Roles and responsibilities related to information security and service delivery are defined by management. Personnel responsibilities include system access, data handling, incident reporting, and compliance with internal policies.

**Security Awareness**

Personnel receive security awareness training as part of onboarding and periodically thereafter. Training covers confidentiality obligations, phishing risks, secure handling of client data, and incident reporting requirements.

### 3.4.4 Procedures

**IT Security Procedures**

IT security procedures govern access management, endpoint security, monitoring, logging, and data protection practices. Procedures are designed to support the Trust Services Criteria in scope.

**Incident Response Procedures**

Incident response procedures require the identification, reporting, investigation, containment, and remediation of security incidents or suspected unauthorized access. Management oversight is applied to incident handling activities.

### 3.4.5 Data

**Client Financial and Tax Data**

The system processes client financial, accounting, and tax-related data as part of service delivery. Data remains under client ownership at all times.

**Data Classification and Handling**

Data is classified based on sensitivity and handled in accordance with internal policies. Access to data is restricted to authorized personnel, and secure transmission and storage practices are enforced. Storage of client data on personal or unauthorized devices is prohibited.

# 4. Control Environment

**Control Environment**

*(Applicable to SOC 2 Type 1 and SOC 2 Type 2)*

The control environment of **Fino Partners Group, Inc.** reflects management's commitment to information security, confidentiality, integrity, and availability of systems used to support service delivery. The control environment establishes the foundation for controls designed to meet the applicable **Trust Services Criteria**.

## 4.1 Governance and Oversight

**Management Responsibilities**

Management is responsible for establishing, maintaining, and overseeing controls related to information security and system operations. Responsibilities include approving security policies, assigning roles and responsibilities, overseeing compliance with internal requirements, and providing direction for the protection of client data and systems.

Management oversight supports the achievement of service commitments and system requirements related to Security, Confidentiality, Processing Integrity, and Availability.

**Security Governance**

Security governance is established through documented policies, defined accountability, and management oversight. Governance structures support consistent application of security controls, monitoring of compliance, and escalation of security-related issues. Management reviews security matters and ensures appropriate response to identified risks or incidents.

## 4.2 Policies and Standards

Fino Partners Group, Inc. has established formal policies and standards designed to govern system access, data protection, confidentiality, and ethical conduct. These policies are communicated to personnel and form the basis for operational security procedures.

**Information Security Policy**

The Information Security Policy defines the organization's approach to protecting systems and information, including access controls, authentication requirements, endpoint security, monitoring, and incident response.

**Acceptable Use Policy**

The Acceptable Use Policy defines responsibilities for the secure and appropriate use of company systems, devices, and networks. The policy restricts unauthorized software, external storage devices, and unapproved system access and establishes expectations for secure remote work.

**Data Protection Policy**

The Data Protection Policy establishes requirements for the classification, handling, storage, transmission, and disposal of sensitive financial and personal information. Access to data is restricted to authorized personnel, and storage of client data on personal or unauthorized devices is prohibited.

**Confidentiality Policy**

The Confidentiality Policy requires personnel to protect client financial, tax, and proprietary information. Employees are required to comply with confidentiality obligations and restrict disclosure of information to authorized business purposes only.

**Code of Conduct**

The Code of Conduct establishes expectations for ethical behavior, compliance with internal policies, and responsible system usage. Personnel are required to report suspected security incidents, policy violations, or unethical behavior.

## 4.3 Risk Assessment

**Security Risk Identification**

Management identifies risks that could reasonably be expected to affect the security, confidentiality, processing integrity, or availability of systems and data. Risk identification considers factors such as system access, remote work arrangements, data handling practices, and threat landscape considerations.

**Risk Mitigation Approach**

Identified risks are addressed through the design of security and operational controls, including access controls, endpoint security, monitoring, incident response procedures, and employee training. Controls are designed to mitigate identified risks and support compliance with the applicable **Trust Services Criteria**.

# 5. Control Activities (SOC 2)

**Control Activities Related to Trust Services Criteria**

*(Applicable to SOC 2 Type 1 and SOC 2 Type 2)*

The control activities of **Fino Partners Group, Inc.** are designed to address risks relevant to the **Trust Services Criteria**—Security, Confidentiality, Processing Integrity, and Availability—by safeguarding systems and data used in service delivery.

## 5.1 Logical and Physical Access Controls

**User Access Management**

Controls are designed to ensure that access to systems and client environments is granted only to authorized personnel based on documented business need. Access requests require management approval, and access is provisioned using unique user accounts. Access is designed to be revoked promptly upon role change or termination.

**Role-Based Access**

Role-based access controls are designed to limit system permissions to those necessary for assigned responsibilities. Privileged access is restricted and granted only when required for operational purposes, consistent with the principle of least privilege.

**Endpoint Security**

Company-managed endpoints are protected through controls designed to reduce the risk of unauthorized access or data exposure. Endpoint controls include device hardening, antivirus protection, restricted administrative privileges, automatic screen locking, and enforcement of company-approved software usage.

## 5.2 System Operations

**Monitoring and Logging**

Controls are designed to monitor system activity and log user access, system events, and security-relevant actions. Logging information supports the detection of anomalous activity and provides evidence for review and investigation.

**Incident Detection and Response**

Incident detection and response controls are designed to identify, report, investigate, and respond to security incidents or suspected unauthorized access. Procedures include incident escalation, containment, remediation, and management oversight of incident resolution.

## 5.3 Change Management

**System and Configuration Changes**

Controls are designed to manage changes to internal systems and configurations that support service delivery. Changes require management authorization and are implemented in accordance with documented procedures. The organization does not implement changes to client-owned systems without client authorization.

## 5.4 Data Protection Controls

**Encryption**

Controls are designed to protect sensitive information through the use of encryption or equivalent safeguards for data transmitted over networks and, where applicable, data stored within approved systems.

**Secure Transmission**

Secure communication channels and approved file-sharing platforms are used for transmitting confidential information. The use of unapproved or insecure transmission methods for client data is restricted.

### Data Retention and Disposal

Controls are designed to retain data only for the period required to support service delivery and contractual obligations. Data disposal procedures are designed to ensure secure deletion or destruction of data when it is no longer required.

## 6. Information and Communication

### Information and Communication

*(Applicable to SOC 2 Type 1 and SOC 2 Type 2)*

The information and communication processes of **Fino Partners Group, Inc.** are designed to support the identification, capture, and communication of information necessary to meet service commitments and system requirements related to the **Trust Services Criteria**.

### Security Communications

The organization has established communication processes to disseminate information security policies, standards, and procedures to personnel. Security-related communications include policy acknowledgments, security awareness guidance, and updates related to identified risks or control requirements. These communications are designed to promote consistent understanding of security responsibilities.

### Incident Reporting

Procedures are designed to enable timely reporting of suspected or confirmed security incidents. Personnel are instructed to report incidents through defined channels, and reported incidents are escalated to appropriate management for investigation and response in accordance with incident response procedures.

### Client Communications

Communication with clients regarding service delivery, security matters, and information requests is conducted through approved and secure communication channels. Client communications related to security incidents or data protection matters are managed in accordance with contractual requirements and established procedures.

## 7. Monitoring Activities

### Monitoring of Controls

*(Applicable to SOC 2 Type 1 and SOC 2 Type 2)*

The monitoring activities of **Fino Partners Group, Inc.** are designed to support the ongoing oversight of controls related to Security, Confidentiality, Processing Integrity, and Availability. Monitoring activities help management identify control deficiencies, security events, or emerging risks that may impact the system.

### Ongoing Security Monitoring

The organization has designed processes to monitor system activity and security-related events. Monitoring activities include the review of logs, alerts, and other security indicators generated by systems, endpoints, and cloud platforms. These activities are intended to detect unauthorized access attempts, anomalous behavior, or potential security incidents in a timely manner.

### Management Review of Security Events

Management is responsible for reviewing identified security events, alerts, and incident reports. Reviews are designed to assess the significance of events, determine appropriate response actions, and ensure that incidents are investigated and addressed in accordance with established procedures. Management oversight supports accountability and continuous improvement of security controls.

# 8. Complementary User Entity Controls

**Complementary User Entity Controls (CUECs)**

*(Applicable to SOC 2 Type 1 and SOC 2 Type 2)*

Certain service commitments and system requirements described in this report assume that user entities implement and maintain specific controls within their own environments. The effectiveness of controls implemented by **Fino Partners Group, Inc.** may depend, in part, on the effective operation of these **Complementary User Entity Controls (CUECs)**.

**Client Security Responsibilities**

User entities are responsible for establishing and maintaining appropriate security controls within their own environments, including:

- Protecting the confidentiality and integrity of client-owned systems and data
- Implementing security policies, procedures, and awareness training for their personnel
- Monitoring their environments for unauthorized access or security incidents
- Complying with applicable legal, regulatory, and contractual security requirements

These responsibilities support the achievement of the Trust Services Criteria related to **Security, Confidentiality, Processing Integrity, and Availability**.

**Client Access Management**

User entities are responsible for administering access to their own systems, applications, and data, including:

- Granting, modifying, and revoking user access to client-owned systems
- Assigning appropriate role-based permissions
- Periodically reviewing access rights for appropriateness
- Securing authentication credentials used by their personnel

The organization's controls assume that client access to systems and data is properly restricted and maintained by user entities.

# 9. Other Information

**Other Information Provided by the Service Organization**

*(Not Covered by the Service Auditor's Opinion)*

The information contained in this section is provided by **Fino Partners Group, Inc.** and is **not part of the service auditor's examination**. Accordingly, the service auditor does not express an opinion or provide any assurance on this information.

This section may include additional background information regarding the organization's services, operational practices, or administrative matters that are not directly related to the service commitments and system requirements based on the applicable **Trust Services Criteria**.

The inclusion of this information is intended solely to provide general context and should not be relied upon by user entities or their auditors for purposes of assessing the design or operating effectiveness of controls.

# 10. Tests of Controls and Results

**Tests of Controls and Results**

*(SOC 2 Type 2 Only)*

This section presents the service auditor's tests of controls and the results thereof for controls described in the system description of **Fino Partners Group, Inc.**. The tests were performed to evaluate whether the controls operated effectively throughout the period **January 1, 2025 to December 31, 2025**, to meet the applicable **Trust Services Criteria for Security, Confidentiality, Processing Integrity, and Availability**.

## 10.1 Description of Tests of Controls

The service auditor performed tests of controls to obtain evidence regarding the operating effectiveness of controls designed to meet the organization's service commitments and system requirements based on the applicable Trust Services Criteria.

Testing procedures were selected based on the nature of the controls, the associated risks, and the frequency of control performance. Tests of controls included, but were not limited to, the following procedures:

- Inquiry of personnel responsible for performing the controls
- Observation of control activities, where applicable
- Inspection of documentation evidencing control performance
- Reperformance of selected control activities

Controls tested included logical and physical access controls, endpoint security controls, monitoring and logging controls, incident detection and response procedures, change management controls, and data protection controls as described in Sections 5 through 7 of this report.

Sampling methodologies and sample sizes were determined by the service auditor based on professional judgment and varied depending on the nature and frequency of each control.

## 10.2 Results of Tests of Controls

The results of the service auditor's tests of controls are presented for each control tested. For each control, the service auditor indicates whether the control operated effectively throughout the period **January 1, 2025 to December 31, 2025**.

Except as noted in the **Identified Exceptions and Management Responses** section below, the controls tested were found to have **operated effectively** to meet the applicable service commitments and system requirements based on the Trust Services Criteria.

## 10.3 Identified Exceptions and Management Responses

Where exceptions were identified during testing, the service auditor documented the nature of the exception and its impact on the related Trust Services Criteria. Management provided responses describing corrective actions taken or planned, where applicable.

If no exceptions were identified, this section may state:

**"No exceptions were identified during the testing of controls for the period January 1, 2025 to December 31, 2025."**

**DAT TIEN NGO** CERTIFIED PUBLIC ACCOUNTANT


License Number: CA065393
datngocpa@gmail.com
Date: January 7, 2026