



SOC 3® Report

Controls Related to Security and Confidentiality

For the Period November 15, 2025 to May 15, 2026

Prepared in accordance with the attestation standards established by the American Institute of Certified Public Accountants



Table of Contents

Independent Service Auditor's Report	1
Assertion of RoundTable Technology, Inc. Management	3
Management's System Disclosures	4
Types of Services Provided	4
Boundaries of the System	4
Principal Service Commitments and System Requirements	9



Independent Service Auditor's Report

To the Management of RoundTable Technology, Inc.
Frisco, Texas

Scope

We have examined RoundTable Technology, Inc.'s (the Company) accompanying assertion titled "Assertion of RoundTable Technology, Inc. Management" (assertion) that the controls within the IT Managed Services System (the System) were effective throughout the period November 15, 2025 to May 15, 2026, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the System to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled "Assertion of RoundTable Technology, Inc. Management" about the effectiveness of controls within the System. When preparing its assertion, the Company is responsible for selecting and identifying in its assertion the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the System.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that the controls within the System were effective throughout the period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted following attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects.

We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent of the Company and to meet our other responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the System were effective throughout the period November 15, 2025 to May 15, 2026, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

MJD Advisors

Waukee, Iowa
October 12, 2026



Assertion of RoundTable Technology, Inc. Management

We, as management of RoundTable Technology, Inc., are responsible for designing, implementing, operating, and maintaining effective controls within the System throughout the period November 15, 2025 to May 15, 2026, to provide reasonable assurance that the Company's service commitments and system requirements relevant to security and confidentiality were achieved. We have described the boundaries of the System in the section titled "Management's System Disclosures" (the System Disclosures), which identifies the aspects of the System covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period November 15, 2025 to May 15, 2026, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Our objectives for the System in applying the applicable trust services criteria are embodied in our service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the System Disclosures.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the period November 15, 2025 to May 15, 2026, to provide reasonable assurance that our service commitments and system requirements were achieved based on the applicable trust services criteria.

Management of RoundTable Technology, Inc.
October 12, 2026

Management's System Disclosures

Types of Services Provided

RoundTable Technology, Inc. provides managed IT services to nonprofits and mission-driven SMBs through the following primary solutions, which are collectively described throughout this description as the IT Managed Services System (the System):

Managed IT Support: Provides continuous access to the Company's support team and includes proactive monitoring and maintenance, patch management, malware protection, documentation, cybersecurity tools, and regular check-ins from an assigned account manager.

Projects: Provides engineering services for major organizational technology changes ranging from scoping, project management, implementation, and documentation.

Strategic Consulting: Provides strategic technology guidance to organizations in a capacity comparable to that of a dedicated technology executive, such as a CIO, CTO, CISO, or CDO, to support strategic decision-making for infrastructure, services, and systems.

The Company is headquartered in Texas and maintains physical office locations in Texas, New York City, and Maine. However, the physical controls associated with these office locations are not within the scope of this description, given sensitive data is either processed or stored in customer systems the Company supports or within cloud services operated by third-party providers, including the Subservice Organizations (providers whose controls are necessary alongside the Company's controls to achieve its service commitments and system requirements), which are responsible for the physical security of their facilities.

This description addresses the data and systems used by the Company to deliver the services that make up the System. Systems and tools used by customers that are outside the Company's control or governance are not within the scope of this description.

Boundaries of the System

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle, such as initiation, authorization, processing, recording, and reporting for the services provided to user entities. The system boundaries do not include instances in which service information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

Infrastructure

The Company's infrastructure is delivered through a software-as-a-service model supported by third-party providers. The Subservice Organizations are responsible for the physical security, environmental protection, and underlying infrastructure of the platforms they provide. The Company is responsible for securely configuring and administering these platforms and the customer systems used to deliver its services.

The categories of third-party services that support the System are summarized below:

Infrastructure and Software - Internal Systems	
Service Category	Description
Productivity and Collaboration	Email, file storage, document collaboration, communication, and video conferencing
Service Delivery	Ticketing, project management, documentation, and remote monitoring and management of endpoints
Security and Monitoring	Endpoint protection, threat detection, vulnerability management, and network protection
Identity and Access	Single sign-on, multi-factor authentication, and credential management
Business Operations	Customer relationship management, human resources, electronic signature, compliance management, and security awareness training

Complementary Subservice Organization Controls

Certain controls of the Subservice Organizations are necessary, in combination with the Company's controls, to provide reasonable assurance that the Company's service commitments and system requirements are achieved. The Company oversees and monitors the Subservice Organizations through its vendor management policies and procedures. The types of controls expected at the Subservice Organizations are as follows.

Complementary Controls	
Criteria	Control
Logical and Physical Access CC6 Series	Authorized users are authenticated, physical and logical access is restricted, and unauthorized access attempts are detected. Access is provisioned and removed based on authorization. Production assets are securely decommissioned and destroyed. Encryption protects data in transit and at rest, by default or as configured by the Company.

Complementary Controls	
Criteria	Control
System Operations CC7 Series	Vulnerability scans and penetration testing are performed periodically. Data center facilities have environmental protections, monitoring, and regular maintenance. Incident response procedures identify, analyze, and remediate events and incidents.
Change Management CC8 Series	System changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.

The examination performed by the independent service auditor did not extend to the policies, procedures, and controls of the Subservice Organizations.

Complementary User Entity Controls

The Company's services use a shared responsibility model. The Company has limited its service commitments to matters for which it is responsible and that it can reasonably achieve on its own. Therefore, complementary user entity controls are not required to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. Customers remain responsible for the security practices within their own environments, as communicated through customer agreements and guidance.

Software

Certain software products are managed by the Company and deployed within customer systems in connection with the services provided. Administration of these systems is either performed by the Company or shared with the customer, and the products are subject to the Company's vendor management program.

Internal AI Tooling

The Company uses third-party AI-enabled tools to support internal productivity, including research, documentation, meeting notes, and other business workflows. No customer-facing AI capability is integrated into the Company's service delivery. The AI meeting tools may process customer meeting recordings when consent is obtained to generate notes and action items. Use of AI tools is governed by the Company's AI acceptable use policy and vendor management program. These tools are not required for the Company's controls to operate effectively and are therefore not included in the service categories above.

People

The Company's organizational structure provides the framework for the management, operation, and security of the System. The table below summarizes the key roles and functional responsibilities of the Company. Due to the Company's size, one individual may serve multiple roles.

Organizational Structure	
Role	Function
President	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities
Leadership Team	Responsible for establishing strategic goals, implementing oversight of the development and implementation of internal control
Virtual CISO / Security Officer	Responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Cyber Team	Cross-functional team responsible for oversight, implementation, and continual improvement of the Information Security Program
Sales	Primary contact with prospective customers and responsible for communicating the Company's service commitments and information about the design and operation of the System and its boundaries
Legal	Responsible for compliance and legal functions of the Company, including external attorneys providing services under management supervision
Human Resources	Responsible for managing the onboarding, performance management, and personnel termination processes
Technical Delivery (Customer Support)	Delivers the services that make up the System through its help desk, onsite support, and project teams. Serves as the primary contact for customer users; accesses and administers customer systems based on assigned responsibilities and least privilege; handles service requests and security alerts through the ticketing system from assignment to closure; maintains customer system documentation; coordinates project-delivery partners on larger projects; and executes customer data retention and deletion processes.
Marketing	Responsible for branding, market awareness, and analyzing service adoption

The Company uses a remote workforce, with personnel located in multiple countries, to manage, operate, and secure the System. Certain personnel are engaged as independent contractors but are subject to the same controls as employees and are treated as personnel throughout this description. The Company also engages project-delivery partners and other contractors for specific projects or periods, subject to its vendor risk assessment process, contractual security requirements, and controls based on their level of access to sensitive information.

Procedures

Procedures are the specific actions undertaken to implement a process, consisting of linked procedures designed to accomplish a particular goal. Policies, which serve as the basis of procedures, are management’s statements of what should be done to meet system objectives and may be documented, explicitly stated in communications, or implied through actions and decisions. The Company maintains a documented Information Security Program that is reviewed and formally approved by management annually, made available to all personnel, and acknowledged by personnel annually. The program addresses acceptable use of technology and artificial intelligence, asset management, backup and disaster recovery, business continuity, change management, contractor security, data classification, protection, and retention, incident response, logging and monitoring, physical security, privacy, risk assessment, vendor management, and vulnerability management.

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners. The following table summarizes the types of data collected by the Company in connection with the System’s services.

Data Type Summary	
Type	Description
Account data	Personally identifiable and administrative information relating to personnel, customers, and other third parties
Customer system documentation	Sensitive customer information such as risk assessments and network diagrams, maintained to support service delivery
Customer credentials	Credentials used to access customer systems in connection with the services provided
Log information	System and activity logs, including metadata, necessary to support and secure the services
Analytics data	Public website traffic and usage data

Access to critical tools is restricted based on the principle of least privilege and requires multi-factor authentication.

Principal Service Commitments and System Requirements

The information presented within the Boundaries of the System was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the objectives that drive the system's operation.

System Requirements

The Company's system requirements are communicated through policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures describe the manual and automated processes required to operate the services provided.

Service Commitments

Service commitments are made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security and confidentiality commitments are communicated through master services agreements, statements of work, and information shared on the Company's website. These commitments match those in the Company's SOC 2 report for the same period.

The following summarizes the Company's principal service commitments:

- A high-level member of management is responsible for establishing procedures for safeguarding customer data (the Security Officer).
- Periodic risk assessments (no less frequently than annually) for appropriateness of safeguards and to make appropriate modifications.
- The Company uses commercially reasonable physical, managerial, and technical safeguards designed to secure data from accidental loss and unauthorized access.
- Security measures including, but not limited to, encryption and password protection for all mobile devices and other equipment with information storage capability to the extent technically feasible.
- Access to critical resources and sensitive information requires multi-factor authentication and is provided based on the principle of least privilege.
- The Company continuously monitors access to its infrastructure.
- The Company has implemented data breach response, disaster recovery, and business continuity protocols.
- Data is maintained and disposed of in accordance with regulatory and customer requirements.