bakertilly

Proprietary & Confidential

Ritter COMMUNICATIONS

Data Technology Center System

SOC 3

Relevant to Security and Availability

AICPA SOC aicpa.org/soc4so SOC for Service Organizations™

FEBRUARY 1, 2025 TO FEBRUARY 28, 2026

Table of Contents

I. Independent Service Auditor's Report

E. Ritter Communications Holdings, LLC
2400 Ritter Drive
Jonesboro, AR 72401

To the Management of E. Ritter Communications Holdings, LLC:

Scope

We have examined E. Ritter Communications Holdings, LLC's accompanying assertion in Section II titled "E. Ritter Communications Holdings, LLC's Assertion" (assertion) that the controls within E. Ritter Communications Holdings, LLC's Data Technology Center System (system) were effective throughout the period February 1, 2025 to February 28, 2026, to provide reasonable assurance that E. Ritter Communications Holdings, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA *Trust Services Criteria*.

Service Organization's Responsibilities

E. Ritter Communications Holdings, LLC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that E. Ritter Communications Holdings, LLC's service commitments and system requirements were achieved. E. Ritter Communications Holdings, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, E. Ritter Communications Holdings, LLC is responsible for selecting, and identifying in its assertion, the applicable trust services 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 controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with 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 that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical 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 controls were not effective to achieve E. Ritter Communications Holdings, LLC's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve E. Ritter Communications Holdings, LLC's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

There are inherent limitations in the effectiveness of 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 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 E. Ritter Communications Holdings, LLC's Data Technology Center System were effective throughout the period February 1, 2025 to February 28, 2026, to provide reasonable assurance that E. Ritter Communications Holdings, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Baker Tilly US, LLP

Seattle, Washington
April 2, 2026

II. E. Ritter Communications Holdings, LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within E. Ritter Communications Holdings, LLC's Data Technology Center System (system) throughout the period February 1, 2025 to February 28, 2026, to provide reasonable assurance that E. Ritter Communications Holdings, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and 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 February 1, 2025 to February 28, 2026, to provide reasonable assurance that E. Ritter Communications Holdings, LLC's service commitments and system requirements were achieved based on the trust services criteria. E. Ritter Communications Holdings, LLC's objectives for the system in applying the applicable trust services criteria are embodied in its 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 Attachment B.

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 February 1, 2025 to February 28, 2026, to provide reasonable assurance that E. Ritter Communications Holdings, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - E. Ritter Communications Holdings, LLC's Description of the Boundaries of Its Data Technology Center System

A. System Overview

1. Services Provided

E. Ritter Communications Holdings, LLC (Ritter) is one of the leading local independent communications providers in the four states it serves. Founded in 1906, Ritter is headquartered in Jonesboro, Arkansas and offers business, wholesale, and residential internet, phone, video, and cloud services in Arkansas, Texas, Tennessee, Missouri, Kentucky, and Louisiana.

Ritter provides communications and backhaul services to over 60,000 customers on its own routers, switches, optical systems and associated network infrastructure spanning six states. Ritter's regional network consists of more than 9,500 miles of dense wavelength division multiplexing (DWDM) systems supporting an MEF Certified routing and switching network. This network provides multiple options to directly connect with more than 10 regional hubs and 18 national hubs including various carrier hotels. Ritter's network also supports its Fiber to The Tower (FTTT) service, wave transport, and Ethernet private line/local area network (LAN) and point-to-point (P2P) services.

Ritter Communications, a private company, has an executive team of chief level officers with an average 20 years of telecommunications experience. Leading the company as Chief Executive Officer, Heath Simpson is a distinguished telecommunications executive with a robust background in strategy, M&A, finance and operations at major national companies, as well as having served as an officer in the US Army Reserve. Heath joined Ritter in 2020 as Chief Financial Officer assuming the role of President and Chief Operating Officer in 2022. He provides strategic oversight for the company and is a strong advocate for security. Grain Management, LLC, a leading investor in the communications sector, is the majority owner of the company in partnership with Ritter and Company. Ritter employs more than 470 people across 13 offices and warehouses to manage and operate their state-of-the-art network.

Serving as the scope of this SOC 2 examination, Ritter offers data center colocation services aiming at helping customers maximize existing technology investments and avoid capital investment expenditures by leveraging Ritter's highly reliable, secure, carrier-class colocation data center services. The data center is supported by a 24x7x365 Network Operations Center (NOC), advanced security and monitoring systems, and sophisticated fire suppression systems. The data center is outfitted with redundant generators with dual fuel sources, automatic transfer switches (ATSs), main switch panels, uninterruptible power supplies (UPSs) and power distribution units (PDUs) and backed by industry-leading service level agreements (SLAs).

2. Infrastructure

The scope of this SOC 2 Type 2 examination covers Ritter's data center facility located at 1765 Mayfield Drive, Jonesboro, Arkansas. Ritter deploys, maintains, and monitors redundant hardware and infrastructure environments within the data center facility to minimize and eliminate single points of failure within the infrastructure supporting environment collocated in the Ritter data center.

The data center is designed to meet or exceed typical geographic threats for its location including exceeding seismic zone 3 building requirements to withstand earthquakes and engineered design to withstand EF3 tornadoes. The exterior of the building includes a reinforced concrete protective wall around the external generator and chiller units and 24x7 video monitoring. The facility has the ability to remain fully functional and within design limits with only one functional chiller unit to increase availability and improve redundancy.

The data center is supported with dual-fuel generator backup power protection, UPS battery backup, fire suppression, a building automation system for environmental monitoring, video monitoring, cardkey-controlled access, mantrap with biometrics access, redundant points of entry, and three-way redundant access to Ritter's fiber backbone.

The data center also has an on-site, 24x7x365 NOC to monitor network and physical security of the data center colocation facility. The Facilities personnel and Data Center Manager monitor alerts from the monitoring systems on a real-time basis. The Data Center and Facilities personnel monitor the health of the environmental systems. In the event of an issue, data center personnel open a ticket, troubleshooting and/or notifying the affected department and/or vendor through a predetermined set of contacts. The tickets are tracked through completion.

Authorized customers also have access to the loading dock and a staging area where they can build or breakdown equipment as needed. Access to the secure data center floor from the staging area is controlled using key card and biometrics. The facility is designed to be carrier grade and meets or exceeds industry standards.

3. Software

Customers fully implement and maintain their own software based on the specific business needs and requirements, to enhance productivity, or for administrative purposes. Ritter has no exposure to or support for any customer-deployed software.

Within the data center environment, Ritter deploys various software to operate and monitor the data center's environmental and security systems. The NOC facility utilizes SolarWinds Orion to monitor the network. Power and cooling systems within the data center are monitored via Simple Network Management Protocol (SNMP) alerts and traps. Remedy and Zoho ticketing systems are used as ticketing systems to track alerts through to resolution. Environmental and physical access within the data center are monitored by dedicated control systems and monitored by Data Center and Facilities personnel.

The NOC uses SolarWinds, Nokia Network Functions Manager for Packet (NFM-P) and Access Management System (AMS) as well as Palo Alto to manage the IP and firewall platforms. Palo Alto firewalls and Intrusion Prevention Systems (IPS) are utilized to protect against Distributed Denial of Service (DDoS) attacks. Since Ritter is an Internet Service Provider (ISP) and provides connectivity utilizing its network, it has the ability to mitigate DDoS attacks without adversely affecting customer connectivity. This DDoS migration is performed by the Nokia Deepfield solution which tightly integrates to the Ritter IP/MPLS core to quickly identify and mitigate attacks.

4. People

Ritter's functional area organizational structure was adopted in late 2022, wherein "Chief Officers" have responsibility for key functions that extend across all of the company's customer types. Ritter is led by the Chief Executive Officer (CEO), who has a leadership team of direct reports comprised of the Chief Technology Officer, Chief Revenue Officer (CRO), and Chief Financial Officer (CFO). These Chief Officers have the ultimate responsibility for the design, development, implementation, operation, maintenance, and monitoring of the system. In addition, the company's Vice President of Human Resources, Vice President of Customer Experience, Vice President of Field Operations, Vice President of Public Affairs and Community Relations as well as the Vice President of Information Technologies, Program Management and Facilities report directly to the CEO. The Vice President of Marketing, the Vice President of Enterprise Sales, and the Vice President of Carrier and Wholesale Services reports to the CRO. The Vice President of Financial Planning & Analysis reports to the CFO. Each data center customer is assigned a Business Account Representative who serves as a conduit between data center tenant needs and Ritter facility operations, design, and implementation.

ORGANIZATIONAL STRUCTURE

Employees have access to an organizational chart through Ritter's intranet portal. Ritter offers hands-on coaching and training to employees, as well as ongoing training opportunities to its managers and leaders.

To help Ritter empower its employees and ensure a positive culture, an internal knowledgebase exists that contains policies, the Ritter Employee Handbook, and other helpful resources that ensure employees are kept abreast of changes to policies and procedures. Employees are informed of material changes to policies and procedures via internal emails.

As part of management's vision to empower employees, and to deliver class leading service through its data center, a Data Center Manager position was created. The Data Center Manager and the Facilities Team oversee all aspects of ongoing data center and building operations including facility infrastructure testing, preventative maintenance, service delivery, quality assurance, and adherence to corporate standards and processes. The Data Center Manager serves as a subject matter expert in data center operations and compliance for Ritter and supports both customers and internal team members.

Key job responsibilities for the Data Center Manager include overseeing installation and commissioning of all new equipment within the data center; maintaining a log of any maintenance discrepancies and leading root cause analysis into any abnormal occurrences within the data center operations; and facilitating security audits and certifications processes for the data center.

JOB DESCRIPTIONS

Ritter has an organizational chart that defines the departments and hierarchical reporting structure, including data center operations. Human Resources (HR) maintains employee job descriptions. Job descriptions are reviewed and updated as needed to ensure continued compliance with Ritter requirements. Job-specific personnel goals are documented for each employee and reviewed by personnel and managers annually.

ACCESS AUTHORIZATION

During the onboarding process, Ritter employees are informed of the guidelines, policies, and security rules that all Ritter employees adhere to. Security Policies are provided during onboarding of new hires, including new employees and contractors. Access to business tools, functions, and Ritter facilities are developed on departmental levels aligned with the specific responsibilities specific to each organizational role, requiring specific approval from managers and/or directors. Ritter employees and contractors execute non-disclosure agreements as part of the onboarding process. Access in general is role-based and aligned to skills, training, knowledge, and need.

Upon hiring, the hiring manager completes a New Hire Checklist, that among other things, outlines security access required for the role and corresponding duties assigned. IT Operations provisions appropriate user accounts, assigns temporary passwords, and sets a requirement for immediate password change upon first sign-in. The individual team member's manager is responsible for keeping IT Operations aware of changes to access needs needed, which are tracked in the same employee New Hire Checklist and used upon role change or de-provisioning of the individual.

During initial onboarding for new data center customers, customers are required to designate a main customer contact. The designated main customer contact is responsible for adding, updating, and removing employees of the customer from the customer's authorized access list. Individuals on a customer's authorized access list enter the data center through the main door and follow all documented security procedures including identity verification by the Data Center Manager or authorized designee using government issued photo identification. The Data Center Manager or authorized designee ensures that the customer or visitor logs into the Visitor Management System (VMS) with the name of the visitor, the date and time of the visit, and then their photo is taken and stored in a digital visitor log after validating that the visitor is on the customer's authorized visitor list.

In the event that a customer needs to add, modify, or remove equipment, monitored access to the loading bay and staging area is provided after identity and authorization verification. For vendors of customers, the main customer contact is required to provide a temporary authorization request via email at least 24 hours prior to the schedule visit or have the completed vendor colocation application form on file.

5. Data

Data controls including security are of the utmost importance to Ritter. Ritter does not de-encrypt customer transmissions and monitors pathing and traffic patterns. Ritter employees are required to review and acknowledge the Security Policy annually.

Ritter does not share customer information to unauthorized internal and external customer personnel. In addition, Ritter customer information is not visible or accessible by any other Ritter tenant or user.

Ritter follows the Data Disposal Policy, and while data center tenants are responsible for their own software and hardware, Ritter obtains signed authorizations from customer representatives in cases where hardware is removed or decommissioned from the data center.

6. Processes and Procedures

GOVERNANCE

Ritter's processes emphasize manageability, security, availability, access, and uptime across all business functions including Network Engineering, Information Technology, NOC, HR, and Finance. Internal policies and documents, including the Ritter Employee Handbook, organizational charts, Information Security Policy, and others are readily available on the employee intranet and employees are informed of any significant changes to policies via company-wide email/notification.

Ritter's data center operations business process and procedures include:

- 24x7 NOC monitoring for health and performance
- Physical and logical access control
- Visitor management process
- Customer onboarding/offboarding
- Employee onboarding/offboarding
- Library of policies and procedures available related to data center security and availability
- Standard operating procedures and checklists
- Preventative maintenance on data center infrastructure
- Change management processes
- IT security and availability policies
- Incident management policies
- Employee handbook policies
- Code of conduct
- Confidentiality agreements
- Hiring and termination policies

INCIDENT RESPONSE PROCESS

Ritter has established procedures for incident response and employees are trained in appropriate reporting and handling of incidents. The Data Center Manager and the Facilities personnel are all trained in appropriate handling of incidents including raising tickets for the appropriate departments to contain and resolve the underlying issue.

Ritter also has a Business Continuity Plan in place to ensure immediate resource engagement and problem resolution. The Business Continuity Plan is reviewed annually and updated to reflect changes in personnel, responsibilities, and procedures, as needed. The Business Continuity Plan is tested annually to ensure personnel are familiar with the procedures. Ritter's standard SLAs for time to restore services is defined within the MSAs and systems are monitored to ensure compliance with defined SLAs.

HIRING

Ritter conducts interviews and background checks for all new employees prior to employment. Interviews are done with one or more members of the hiring team for prospective new hires, two or more references are required, and employment verification from the previous employer is conducted. A background check and a drug test are conducted after an offer letter has been signed, and the completion of both tests is required prior to the employee start date.

SECURITY TRAINING

Security awareness training is provided to all Ritter employees. The training covers multiple topical subjects including: physical security, access controls, and cybersecurity. Mandatory security training occurs upon hiring and is repeated annually.

TERMINATIONS

HR, Facilities, and IT have policies and close collaboration to ensure that user provisioning and deprovisioning occur in a timely manner. If employee or tenant termination is required, the request is treated urgently, and access is removed for all systems and facilities as outlined in a Termination Checklist.

Attachment B – Principal Service Commitments and System Requirements

Ritter designs its processes and procedures related to its Data Technology Center System to meet its objectives based on the service commitments that Ritter makes to customers, the laws and regulations that govern the provision of colocation services, and the financial, operational, and compliance requirements that Ritter has established for the services. Security commitments to customers are documented and communicated in Master Services Agreements (MSAs) and other customer agreements.

Ritter establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Ritter's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. Policies centered around logical and physical access to protected information are designed to limit access based on roles and permissions so that the principle of least access is consistently applied across the environment. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the management and operation of the data center.

Ritter's service commitments around system availability are documented within its MSA with its customers. Redundant infrastructure as well as system monitoring procedures are designed to ensure compliance with the contractually agreed upon service level agreements. Internal policies, and procedures are designed, developed, and operated in order to support Ritter's availability commitments while continuing to maintain a focus on security.