

Softdocs

Softdocs SC, LLC

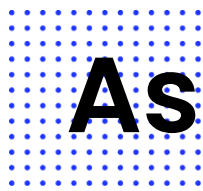
System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust Services Criteria for the Security, Availability, and Confidentiality Categories for the Period of August 1, 2024, through July 31, 2025.



Table of Contents

- Assertion of Softdocs SC, LLC Management..... 1
 - Assertion of Softdocs SC, LLC Management..... 2
- Independent Service Auditor’s Report..... 3
 - Independent Service Auditor’s Report..... 4
 - Scope..... 4
 - Service Organization’s Responsibilities..... 4
 - Service Auditor’s Responsibilities..... 4
 - Inherent Limitations..... 5
 - Opinion..... 5
- Softdocs SC, LLC’s Description of Its Enterprise Content Management Solution System..... 6
 - Section A: Softdocs SC, LLC’s Description of the Boundaries of Its Enterprise Content Management Solution System..... 7
 - Services Provided..... 7
 - Infrastructure 7
 - Software 9
 - People 10
 - Data 10
 - Processes and Procedures..... 11
 - Section B: Principal Service Commitments and System Requirements..... 13
 - Regulatory Commitments..... 13
 - Contractual Commitments..... 13
 - System Design..... 13



Assertion of Softdocs SC, LLC Management

CONFIDENTIAL

Assertion of Softdocs SC, LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Softdocs SC, LLC's enterprise content management solution system (system) throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Softdocs SC, LLC's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in section 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 August 1, 2024, to July 31, 2025, to provide reasonable assurance that Softdocs SC, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, 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*). Softdocs SC, 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 section 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 August 1, 2024, to July 31, 2025, to provide reasonable assurance that Softdocs SC, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.



Independent Service Auditor's Report

CONFIDENTIAL

Independent Service Auditor's Report

Adam Park
CEO
Softdocs SC, LLC
807 Bluff Rd
Columbia, SC 29201

Scope

We have examined Softdocs SC, LLC's accompanying assertion titled "Assertion of Softdocs SC, LLC Management" (assertion) that the controls within Softdocs SC, LLC's enterprise content management solution system (system) were effective throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Softdocs SC, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, 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*).

Service Organization's Responsibilities

Softdocs SC, LLC is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Softdocs SC, LLC's service commitments and system requirements were achieved. Softdocs SC, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Softdocs SC, 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 whether 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 American Institute of Certified Public Accountants. 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.

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 Softdocs SC, 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 Softdocs SC, 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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.

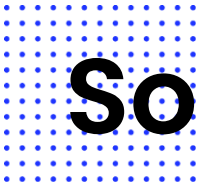
Opinion

In our opinion, management's assertion that the controls within Softdocs SC, LLC's enterprise content management solution system were effective throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Softdocs SC, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

September 8, 2025



Softdocs SC, LLC's Description of Its Enterprise Content Management Solution System

Section A: Softdocs SC, LLC's Description of the Boundaries of Its Enterprise Content Management Solution System

Services Provided

Softdocs SC, LLC (Softdocs) is a remote enterprise Software-as-a-Service (SaaS) company that is committed to serving higher education, K-12 institutions, and state and local government through Etrieve, an enterprise content management (ECM) platform. With a 25-year history, the organization is dedicated to promoting educational and governmental equity.

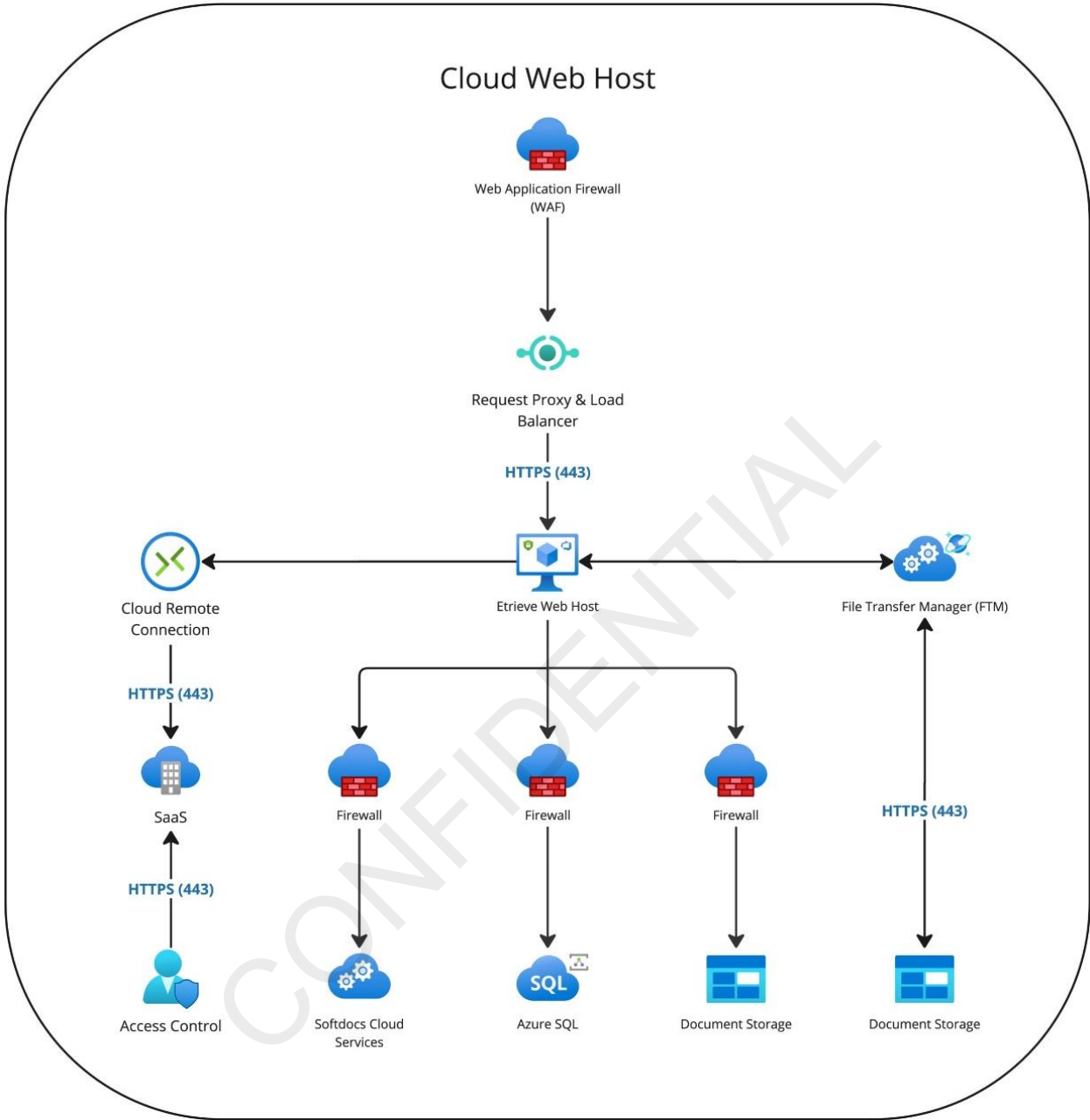
The cloud-deployed, scalable Etrieve platform enables organizations to modernize operations and drive organizational success. Etrieve is a web-based SaaS product used by educational institutions and state and local governments and is an enterprise content management platform. The platform is cloud-based and scalable, allowing organizations to modernize their document flow processes and complete various actions, including scanning and system administration, in a single browser window on any device without needing locally installed software.

Services include:

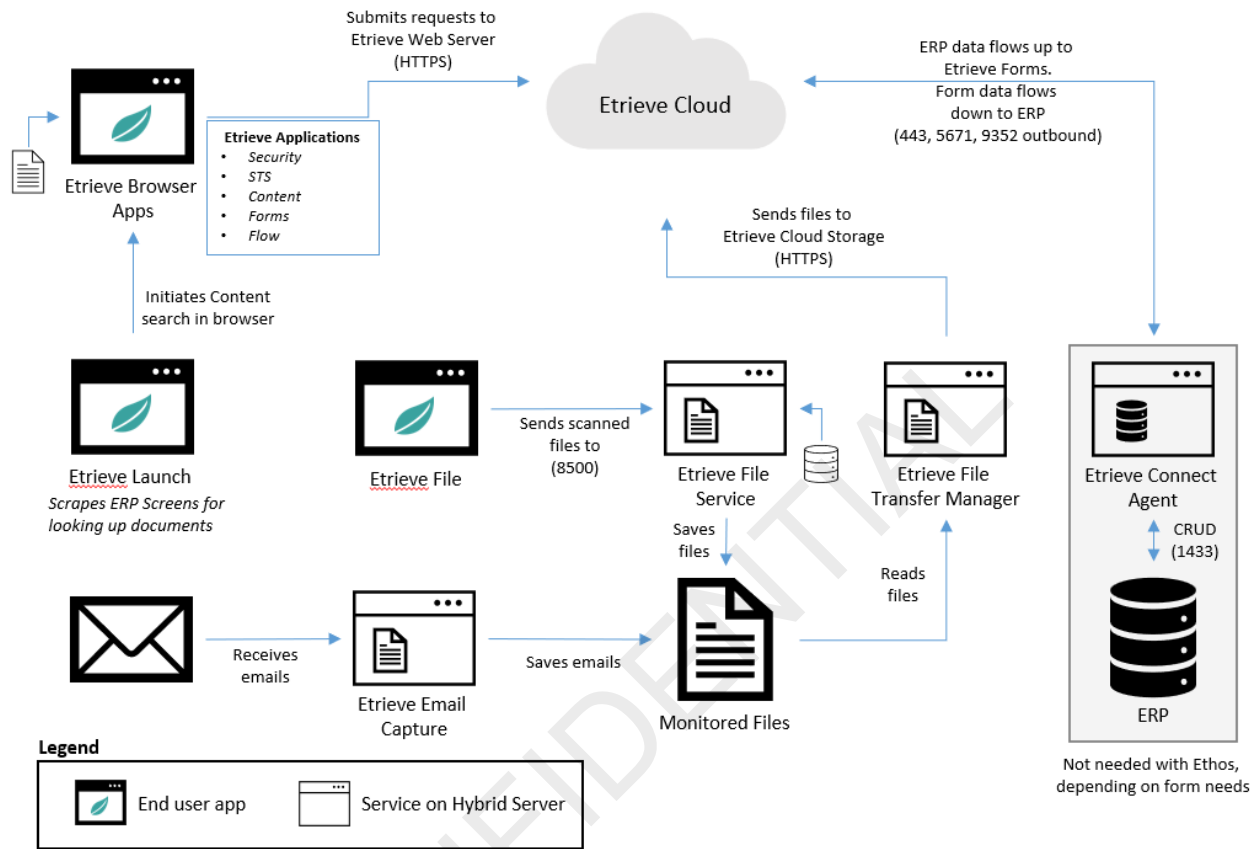
- Cloud infrastructure provisioning, administration, and management
- Discovery and requirements gathering
- Configuration assistance
- Migration assistance, including moving documents from a customer's legacy system into Etrieve or building forms and workflows used in a legacy system in Etrieve
- Administration and end-user product training
 - Standard and custom-tailored offerings
- Custom forms and workflow development
- Custom print output template designs
- Planning and implementation
- Project management
- General Support
- Managed Services
 - Standard services agreements allowing for outsourcing system administration and expansion
- Tax Form Processing (outsourcing)

Infrastructure

The organization develops network diagrams to depict the structure and topography of the network infrastructure. Data flow is shown, along with connection points and secure communication channels.



Etrieve Applications and Data Flow



Software

The organization maintains a software inventory that documents all software downloaded and used by the company. The list outlines the following information for each entry:

- Name
- Version
- Vendor
- Function

Critical software used by the organization includes the following:

- Azure DevOps
- Burp Suite
- ConnectWise
- CPQ (Salesforce Integration)
- CrowdStrike Falcon
- Datadog
- GitHub Copilot
- Microsoft 365
- NinjaOne
- Salesforce
- Snyk
- Sophos

People

Softdocs governance is built upon a framework that integrates leadership visibility, policy discipline, organizational accountability, and cultural consistency. The organizational structure is mapped within a company organization chart, which is updated regularly. This provides clarity for reporting lines and roles across critical functions. The Senior Leadership Team, shown below, ensures governance and direction.



The Board of Directors, which includes both investor representatives and former company owners, meets quarterly to oversee strategy, risk, and organizational performance. The Chief Executive Officer (CEO) maintains direct one-on-one communication with board members and investor representatives from Ridgmont Equity Partners, aligning the company's operational posture with its strategic trajectory.

Leadership defines annual corporate goals, communicated company-wide through quarterly All Hands meetings and reinforced in department meetings, where performance progress and tactical alignment are discussed. Weekly senior leadership meetings review detailed key performance indicators (KPIs)—ranging from sales pipeline health, client onboarding activity, marketing lead sources, and employee sentiment—enabling real-time visibility and course corrections.

Data

Softdocs has a range of measures designed to protect systems, data, and infrastructure from threats and unauthorized access. Access to customer systems is granted on a case-by-case basis and must be logged, tracked, and revoked after use, with monthly audits conducted to validate adherence. Antivirus and anti-malware defenses include multiple layers such as endpoint protection, firewall controls, real-time monitoring,

and automated updates across all devices and environments, with incident response procedures for both internal events and customer-facing breaches.

Encryption protocols are applied to data in transit and at rest, while audit logging captures activity such as logins, data access, and account changes, with retention policies and regular reviews in place. Staff are required to follow secure file sharing and data handling practices, particularly when dealing with personal and health-related information. Separation of duties and least privilege principles restrict system access to only what is necessary for each role, with tracking mechanisms integrated into change and onboarding workflows.

The organization maintains data disposal procedures, which emphasize secure handling, controlled access, and documented destruction of physical and digital media. Drives removed from RAID arrays are stored in a locked closet accessible only to IT and executive teams before being destroyed through multi-pass data erasure software and physical dismantling. The company prohibits storing sensitive customer data on endpoint devices and applies classified handling and transport protections to all removable storage, including encryption per FIPS 140-2 standards. Data disposal follows defined retention schedules, with physical documents shredded and digital files erased to prevent reconstruction, and exceptions require leadership approval or may be subject to legal holds.

For cloud environments like Microsoft Azure, Softdocs adheres to the National Institute of Standards and Technology (NIST) SP 800-88 protocols using approved tools for logical media sanitization and relies on Azure's destruction services when hardware must be retired. Media sanitization procedures are tested annually, and all activities related to access and destruction are audited monthly to maintain alignment with operational and regulatory controls.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices
- Retrieve cloud virtual machine and database backup and restoration

- Business continuity
- Disaster recovery
- Cloud server hardening procedure

CONFIDENTIAL

Section B: Principal Service Commitments and System Requirements

Regulatory Commitments

The organization also aims to comply with the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), and Fair Debt Collection Practices Act (FDCPA) standards as applicable to meet client needs. A privacy notice is maintained to communicate data processing, handling, retention, and disposal to clients.

Contractual Commitments

Customer contracts are used to define the terms of service and contain a description of the project for implementation, deliverables, testing, training, and support. A master services agreement (MSA) is used to define information related to confidentiality, security, and client obligations, including user administration and notification of security incidents. Additionally, the statement of work (SOW) outlines Softdocs and Customer responsibilities along with time estimates, and a service-level agreement (SLA) is used to define information regarding management of the Etrieve Cloud environment, including data backup and retention, restoration, disaster recovery, business continuity and availability, traditional and emergency change management, compliance, security, and notifications.

System Design

Softdocs designs its enterprise content management solution system to meet its regulatory and contractual commitments. These commitments are based on the services that Softdocs provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Softdocs has established for its services. Softdocs establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Softdocs' system policies and procedures, system design documentation, and contracts with clients.