SRS ACQUIOM

linford & co llp cpa firm



VIRTUAL DATA ROOM

SOC 3

REPORT ON CONTROLS RELEVANT TO SECURITY, PROCESSING INTEGRITY, AVAILABILITY, AND CONFIDENTIALITY

NOVEMBER 1, 2024 TO OCTOBER 31, 2025

SRS Acquiom Inc.

Report on SRS Acquiom's Description of Its Virtual Data Room and on Its Controls Relevant to Security, Availability, and Confidentiality

Table of Contents

Description **Page**

Section I – Report of Independent Auditors **1**

Section II – Assertion of SRS Acquiom's Management **3**

Section III – SRS Acquiom's Description of Its Virtual Data Room **4**

Overview of Operations 4

Principal Service Commitments and System Requirements 6

Complementary Subservice Organization Controls (CSOC) 7

SRS Acquiom's Complementary User Entity Controls (CUEC) 8

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Report of Independent Auditors

The Board of Directors of SRS Acquiom Inc. (together with its subsidiaries, "SRS Acquiom"):

Scope

We have examined SRS Acquiom's accompanying assertion titled "Assertion of SRS Acquiom's Management" (assertion) that the controls within SRS Acquiom's Virtual Data Room (system) were effective throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that SRS Acquiom'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

SRS Acquiom 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 SRS Acquiom's service commitments and system requirements were achieved. SRS Acquiom has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SRS Acquiom 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 (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 service organization's service commitments and system requirements.
- ✓ Assessing the risks that controls were not effective to achieve SRS Acquiom's service commitments and system requirements based on the applicable trust services criteria.

- ✓ Performing procedures to obtain evidence about whether the controls within the system were effective to achieve SRS Acquiom'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 SRS Acquiom's Virtual Data Room were effective throughout the period November 1, 2024 to October 31, 2025 to provide reasonable assurance that SRS Acquiom's service commitments and system requirements were achieved based on the applicable trust services criteria fairly stated, in all material respects.

linford&co llp

November 6, 2025
Denver, Colorado

SRSACQUIOM

303.648.4085
sales@srsacquiom.com

950 17th Street
Suite 1400
Denver, CO 80202

Section II – Assertion of SRS Acquiom's Management

November 6, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within SRS Acquiom's Virtual Data Room (system) throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that SRS Acquiom'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*). Our description of the boundaries of the system is presented in Section III, and it 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 1, 2024 to October 31, 2025, to provide reasonable assurance that SRS Acquiom's service commitments and system requirements were achieved based on the applicable trust services criteria. SRS Acquiom'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 III.

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 1, 2024 to October 31, 2025, to provide reasonable assurance that SRS Acquiom's service commitments and system requirements were achieved based on the applicable trust services criteria.

Lon LeClair
Chief Operations Officer

Section III – SRS Acquiom's Description of Its Virtual Data Room

Overview of Operations

Overview of the Organization

Founded in 2007, SRS Acquiom invented professional shareholder representation in private company mergers and acquisitions (M&A) and has since expanded its services to include M&A payments, escrow administration, loan agency services, and professional file sharing portal. The more than 200 experts at SRS Acquiom—in forensic accounting, finance, tax, intellectual property, litigation and dispute resolution, technology, customer support, and payment operations—work together to safeguard the interests of more than 540,000 selling shareholders, including over 500 of the world's top venture capital and private equity firms.

Description of the Virtual Data Room

Virtual Data Room (VDR) is a cloud file-sharing and file-storage solution that allows an administrative user to upload different types of files that are made available to parties invited by that user. The invited parties are granted different permissions by the owner that allow them to perform various tasks such as viewing, downloading, printing, and editing the files stored in the VDR. VDR uses enterprise grade data security to make sure there is confidentiality and availability in all data that is stored. Additionally, transferring large batches of files at once is an option using intuitive auto-indexing.

Components of the System Used to Provide the Services

The system used by SRS Acquiom to deliver the VDR services is comprised of a combination of components that includes the products and processing, but also extends to the underlying infrastructure, subservice organization's services supporting the platform, the Company's employees and contractors, as well as the policies and procedures followed to maintain the security, availability, and confidentiality of the SRS Acquiom services and client data. The following is a summary of the components that comprise the offering. Specific process and controls relevant to the security, availability, and confidentiality criteria are described in the remainder of this section of the report.

Infrastructure

SRS Acquiom has a hybrid workforce with its primary office located in Denver, CO. SRS Acquiom relies on a subservice organization to provide IT/Engineering infrastructure resources for the services provided.

Subservice Organization: SRS Acquiom uses a subservice organization to achieve operating efficiency and to obtain specific expertise. The following is the principal subservice organization used by SRS Acquiom for the VDR:

- ✓ **AWS** – AWS hosts SRS Acquiom's Virtual Data Room, in addition to providing other supporting services such as backups and monitoring. AWS undergoes an annual Type II SOC 2 examination and the report may be obtained directly from them. SRS Acquiom obtains and reviews the SOC 2

report provided by AWS related to their hosting services to determine whether controls are designed and operating effectively at AWS. Additionally, any listed complementary user entity controls in the AWS SOC report are also reviewed and addressed by SRS Acquiom.

Software

SRS Acquiom's VDR are enabled by its privately owned applications, and the use of reputable and SOC examined third party tools and applications. The VDR are supported by SRS Acquiom's applications, systems, and tools. The SRS Acquiom applications are run on Linux based systems and are developed and maintained by SRS Acquiom's IT personnel and third-party resources. Role-based access controls (RBAC) govern the capabilities employees and users can execute within the SRS Acquiom applications and tools.

People

SRS Acquiom has a staff of personnel organized into functional areas so that personnel understand their responsibilities within the organization.

Data

Client data is stored within SRS Acquiom's production database instances in their colocation facilities. SRS Acquiom has implemented security controls to protect the confidentiality of the data. Client data within the databases is encrypted at rest. Additionally, all data transfers between users and SRS Acquiom are secured using Transport Layer Security (TLS) and industry-standard encryption.

Processes and Procedures

SRS Acquiom has established and maintains security policies and procedures over the VDR. SRS Acquiom makes these internal policies and procedures, including security policies, available to its personnel on its internal shared drives to provide direction regarding their responsibilities related to the functioning of internal control.

(The remainder of this page is left blank intentionally.)

Principal Service Commitments and System Requirements

SRS Acquiom designs its processes and procedures to meet objectives for its VDR. Those objectives are based on the service commitments that SRS Acquiom makes to user entities and the compliance requirements that SRS Acquiom has established for their services.

Security, confidentiality, and availability commitments to user entities are documented and communicated in their customer agreements, as well as in the description of the service offering provided online. Security, confidentiality, and availability commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the Virtual Data Room are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production infrastructure and client data.
- Segregation of client data.
- Data backups.
- Monitoring of system performance metrics and critical application services.
- Availability and system uptime.

SRS Acquiom establishes operational requirements that support the achievement of security, confidentiality, and availability commitments and other system requirements. Such requirements are communicated in SRS Acquiom's system policies and procedures, privacy policy, 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 networks are managed, and how personnel are hired and trained.

(The remainder of this page is left blank intentionally.)

Complementary Subservice Organization Controls (CSOC)

SRS Acquiom's controls related to the VDR cover only a portion of the overall internal control for each user entity of SRS Acquiom. It is not feasible for the applicable trust service criteria related to the VDR to be achieved solely by SRS Acquiom. Therefore, each user entity's internal controls must be evaluated in conjunction with SRS Acquiom's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described as follows:

	AWS Complementary Subservice Organization Controls
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.
3.	The subservice organization is responsible for maintaining the availability of the hosted environments 24/7/365.
4.	The subservice organization is responsible for managing and resolving security and availability incidents related to the data center facility in a timely manner.

(The remainder of this page is left blank intentionally.)

SRS Acquiom's Complementary User Entity Controls (CUEC)

The VDR provided by SRS Acquiom for user entities and the controls at SRS Acquiom cover only a portion of the user entity's overall system of internal control. It is not feasible for the applicable trust services criteria related to the VDR to be achieved solely by SRS Acquiom. Therefore, each user entity's internal control must be evaluated in conjunction with SRS Acquiom's controls, taking into account the related complementary user entity controls identified under each control criteria, where applicable.

This section highlights additional control activities that SRS Acquiom believes should be considered and/or present at each user entity. Each user entity must evaluate its own system of internal control to determine if the following controls are in place. User auditors should consider whether the following controls have been placed in operation at user organizations:

	Complementary User Entity Controls
1.	It is the client's responsibility to keep their unique username and password private and not share them with anyone else.
2.	User entities are responsible for restricting access to their data in their possession to only authorized individuals and obtaining confidentiality agreements as needed.
4.	User entities are responsible for maintaining the confidentiality of their data while it is in their possession.
5.	User entities are responsible for monitoring that their methods of delivering data to SRS Acquiom conforms with their security and confidentiality requirements.

(The remainder of this page is left blank intentionally.)