



**REPORT ON ACCELYA US, INC.'S DESCRIPTION OF ITS airRM SYSTEM AND ON THE SUITABILITY
OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY,
AVAILABILITY, AND CONFIDENTIALITY**

**Pursuant To Systems and Organization Controls (SOC) 2 Type II Report
For the period October 01, 2023 to September 30, 2024**

Table of Contents

SECTION 1 MANAGEMENT ASSERTION OF ACCELYA US, INC.	3
SECTION 2 INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT	7
SECTION 3 DESCRIPTION OF THE airRM SYSTEM BY SERVICE ORGANIZATION	12
Accelya US, Inc.'s Description of airRM System	13
Scope and Boundaries of the System	13
Company Background	13
Services Provided	13
Principal Service Commitments and System Requirements	14
System Incidents	15
Components of the System Used to Provide the Services	15
Infrastructure	15
Software	16
People	17
Data	18
Description of the Controls Relevant to the Security, Availability, and Confidentiality Trust Services Categories	19
Description of the Additional Controls Relevant to the Availability Trust Services Category	24
Description of the Additional Controls Relevant to the Confidentiality Trust Services Category	24
Complementary Subservice Organization Controls	24
User Entity Responsibilities	26
SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS AND TEST RESULTS	27
CC1.0 Control Environment	29
CC2.0 Communication and Information	42
CC3.0 Risk Assessment	51
CC4.0 Monitoring Activities	56
CC5.0 Control Activities	60
CC6.0 Logical And Physical Access Controls	64
CC7.0 System Operations	87
CC8.0 Change Management	102
CC9.0 Risk Mitigation	106
Additional Criteria for Availability	112
Additional Criteria for Confidentiality	117
LIST OF ABBREVIATIONS	122

SECTION 1 MANAGEMENT ASSERTION OF ACCELYA US, INC.




Accelya US, Inc.
790 NW 107 Ave, Suite 400
Miami, FL, 33172
United States of America

Date: December 20, 2024

ASSERTION OF ACCELYA US, Inc

We have prepared the accompanying description of Accelya US, Inc.'s (Accelya or service organization) airRM system titled "Accelya US, Inc.'s Description of its airRM System" throughout the period October 1, 2023, to September 30, 2024, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 [®]Report, in AICPA Description Criteria. The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Accelya's system, particularly information about system controls that Accelya has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality, set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Accelya uses a subservice organization to perform hosting and operation center services. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Accelya, to achieve Accelya's service commitments and system requirements based on the applicable trust services criteria. The description presents Accelya's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Accelya's controls. The description does not disclose the actual controls at the subservice organization.



The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Accelya, to achieve Accelya's service commitments and system requirements based on the applicable trust services criteria. The description presents Accelya's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Accelya's controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents Accelya's airRM system that was designed and implemented throughout the period October 1,2023, to September 30, 2024, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period October 1,2023, to September 30, 2024, to provide reasonable assurance that Accelya's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Accelya's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period October 1,2023, to September 30, 2024, to provide reasonable assurance that Accelya's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Accelya's controls operated effectively throughout that period.

Accelya states in the description of its airRM system that:

S.No	Control Activity
1	Access to in-scope system components requires documented access request form and manager approval prior to access being provisioned.
2	User IDs are removed from the system components based on an authorized request from the employee's manager as per defined procedure.
3	The Human Resources department sends communication to the respective department as soon as a resource is terminated to remove access. Access is removed based on the communication.
4	Management performs a quarterly user access cleanup to remove user accounts that have been inactive or no longer need access.

5	Employee workstation/laptop hard drives are encrypted.
6	Antivirus software is installed on production machines and configured to receive regular updates, scan for inappropriate files, and notify management of potential issues.
7	Management is monitoring backups failure manually. Failures are tracked to closure.
8	DR plans have been developed, updated, and tested.

However, as noted in Section IV of this report, the controls related to the user access review and provisioning process, information transmission and movement process, change control process, environmental protections and backup process including test recovery plans were not operating effectively throughout the period October 1, 2023, to September 30, 2024. As a result, controls did not provide reasonable assurance that Service Organization's controls were achieved based on:

- Criterion CC6.2, "Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized."
- Criterion CC6.3, "The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives."
- Criterion CC6.7, "The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives."
- Criterion CC6.8, "The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives."
- Criterion A1.2, "The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives."
- Criterion A1.3, "The entity tests recovery plan procedures supporting system recovery to meet its objectives."

Signature



Sam Butler
Chief Information Security Officer

SECTION 2 INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

Independent Service Auditor's Report

To:

Management of Accelya US, Inc.

Scope

We have examined Accelya US Inc. (hereinafter referred as 'Accelya' or 'Service Organization') accompanying description titled "Accelya's System Description of its airRM System" for the services provided to the user entities throughout the period October 1, 2023, to September 30, 2024, in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA Description Criteria and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2023 to September 30, 2024 to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*, in AICPA Trust Services Criteria.

Accelya uses subservice organizations to perform certain services. A list of these subservice organizations and the services performed is provided in the following table.

Subservice Organization	Services Performed
Amazon Web Services, Inc. (AWS)	Third-party cloud hosting services for the airRM system.
Cyderes, LLC	Third-party security operations center services.
Equinix, Inc	Third-party data center hosting services for the Company's network services.

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Accelya, to achieve Accelya's service commitments and system requirements based on the applicable trust services criteria. The description presents Accelya's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Accelya's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Accelya, to achieve Accelya's service commitments and system requirements based on the applicable trust services criteria. The description presents Accelya's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Accelya's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Accelya 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 Accelya's system service commitments and system requirements were achieved. Accelya has provided the accompanying assertion titled "Assertion of Accelya Management" about the description and the suitability of the design and operating effectiveness of controls stated therein. Accelya is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards issued by American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and Accelya's system 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 the controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria.
- Testing the operating effectiveness of the 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

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and 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.

Description of Tests of Controls

The specific controls we tested and the nature timing, and results of those tests are listed in section 4.

Basis for Qualified Opinion

Accelya states in the description of its airRM system that:

S.No	Control Activity
1	Access to in-scope system components requires documented access request form and manager approval prior to access being provisioned.
2	User IDs are removed from the system components based on an authorized request from the employee's manager as per defined procedure.
3	The Human Resources department sends communication to the respective department as soon as a resource is terminated to remove access. Access is removed based on the communication.
4	Management performs a quarterly user access cleanup to remove user accounts that have been inactive or no longer need access.
5	Employee workstation/laptop hard drives are encrypted.
6	Antivirus software is installed on production machines and configured to receive regular updates, scan for inappropriate files, and notify management of potential issues.
7	Management is monitoring backups failure manually. Failures are tracked to closure.
8	DR plans have been developed, updated, and tested.

However, as noted in Section IV of this report, the controls related to the user access review and provisioning process, information transmission and movement process, change control process, environmental protections and backup process including test recovery plans were not operating effectively throughout the period October 1, 2023, to September 30, 2024. As a result, controls did not provide reasonable assurance that Service Organization's controls were achieved based on:

- Criterion CC6.2, "Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized."
- Criterion CC6.3, "The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives."
- Criterion CC6.7, "The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives."
- Criterion CC6.8, "The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives."
- Criterion A1.2, "The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives."
- Criterion A1.3, "The entity tests recovery plan procedures supporting system recovery to meet its objectives."

Opinion

In our opinion, except for the matter referred to in the preceding paragraph, in all material respects:

- a. the description presents Accelya's airRM System that was designed and implemented throughout the period October 1, 2023, to September 30, 2024, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Accelya's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Accelya's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Accelya's system service commitments and system requirements were achieved based on the applicable trust services criteria and if complementary subservice organization controls and complementary user entity controls assumed in the design of Accelya's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Accelya, user entities of Accelya's airRM system during some or all of the period October 1, 2023, to September 30, 2024, business partners of Accelya subject to risks arising from interactions with the hybrid cloud product, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

BDO INDIA LLP

December 20, 2024
BDO India LLP
Gurugram, Haryana