Report on TrackVia, Inc.’s TrackVia Software-as-a-Solution (SaaS) System Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 2021 to May 31, 2022

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor's Report 3

Section 2

Assertion of TrackVia, Inc. Management 6

Attachment A

TrackVia, Inc.'s Description of the Boundaries of Its TrackVia Software-as-a-Solution (SaaS) System 8

Attachment B

Principal Service Commitments and System Requirements 15

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: TrackVia, Inc. ("TrackVia")

Scope

We have examined TrackVia's accompanying assertion titled "Assertion of TrackVia, Inc. Management" (assertion) that the controls within the TrackVia Software-as-a-Solution (SaaS) System (system) were effective throughout the period January 1, 2021 to May 31, 2022, to provide reasonable assurance that TrackVia'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*).

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

Service Organization's Responsibilities

TrackVia 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 TrackVia's service commitments and system requirements were achieved. TrackVia has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, TrackVia 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 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 TrackVia'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 TrackVia'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 examination 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 the TrackVia Software-as-a-Solution (SaaS) System were effective throughout the period January 1, 2021 to May 31, 2022, to provide reasonable assurance that TrackVia's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of TrackVia's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
August 10, 2022

Section 2

Assertion of TrackVia, Inc. Management

950 17th Street
Suite 2000
Denver, CO 80202

800.673.3302
TrackVia.com

Assertion of TrackVia, Inc. ("TrackVia") Management

We are responsible for designing, implementing, operating and maintaining effective controls within TrackVia's Software-as-a-Solution (SaaS) System (system) throughout the period January 1, 2021 to May 31, 2022, to provide reasonable assurance that TrackVia'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 attachment A and identifies the aspects of the system covered by our assertion.

TrackVia uses subservice organizations for data center colocation and integration services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TrackVia, to achieve TrackVia's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of TrackVia's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021 to May 31, 2022, to provide reasonable assurance that TrackVia'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*) if complementary subservice organization controls assumed in the design of TrackVia's controls operated effectively throughout that period. TrackVia'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 January 1, 2021 to May 31, 2022, to provide reasonable assurance that TrackVia's service commitments and system requirements were achieved based on the applicable trust services criteria.

TrackVia, Inc.

Attachment A

TrackVia, Inc.’s Description of the Boundaries of Its TrackVia Software-as-a-Solution (SaaS) System

Type of Services Provided

TrackVia, Inc. (“TrackVia” or “the Company”) is a software-as-a-solution (SaaS) provider. TrackVia produces a low-code application building platform with modern work management capabilities that allows businesses to build applications that streamline and automate critical operational workflows and processes.

The boundaries of the system in this section details the TrackVia SaaS. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the TrackVia SaaS are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the TrackVia SaaS.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the TrackVia SaaS. The Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the TrackVia SaaS architecture within AWS to ensure the availability, security, and resiliency requirements are met.

The TrackVia SaaS is hosted and operated on AWS in multiple regions and availability zones. Below is a list of services leveraged by AWS to provide the TrackVia SaaS:

Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Infrastructure-as-a-service (IaaS)	The Company leverages several AWS services to build, run, and operate the TrackVia SaaS. These services include Amazon Elastic Compute Cloud (Amazon EC2), Amazon Aurora databases, Amazon Simple Store Service (Amazon S3), Amazon S3 Glacier storage, Elastic Load Balancing, Firewall Security, Amazon Route 53 Domain Name System (DNS), Amazon CloudFront content delivery network (CDN), AWS Identity and Access Management, monitoring, logging, and security services.

Infrastructure		
Hardware	**Type**	**Purpose**
Application Servers	Web Servers	TrackVia SaaS utilizes application servers as the primary servers for application logic.
Routers	Web Servers	TrackVia SaaS utilizes routers for load balancing.

Software

Software consists of the programs and software that support the TrackVia SaaS (operating systems [OSs], middleware, and utilities). The TrackVia SaaS is web, Android, iOS, and application programming interface (API) enabled. The list of software and ancillary software used to build, support, secure, maintain, and monitor the TrackVia SaaS include the following applications:

Software		
Software	**Type**	**Purpose**
AWS	IaaS	The Company leverages several AWS services to build, run, and operate the TrackVia SaaS. These services include Elastic Messaging and Queuing, AWS Lambda, and Amazon Elastic Kubernetes Service (Amazon EKS).
iOS Software Development Kit (SDK)	Mobile	The TrackVia SaaS uses the iOS SDK as the OS development platform.
Android SDK	Mobile	The TrackVia SaaS utilizes the Android SDK as the Android development platform.
Workato	SaaS	The TrackVia SaaS is integrated with Workato to provide advanced integrations capabilities.
SendGrid	SaaS	The TrackVia SaaS is integrated with SendGrid to provide advanced email capabilities.

People

The Company develops, manages, and secures the TrackVia SaaS via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.

People	
Group/Role Name	**Function**
Production Operations	Responsible for the overall health of the TrackVia SaaS. Production Operations has implemented security information and event management (SIEM) and monitoring tools to monitor system health, performance, high availability, and disaster recovery.
Information Security	Responsible for managing access controls and the security of the production environment.
Engineering	Responsible for the development, testing, and maintenance of code for the TrackVia SaaS.
Product Management	Responsible for overseeing the product life cycle, including adding new features.
Customer Support	Responsible for working with customers, answering questions, and providing technical support.
Networking Team	Responsible for monitoring network devices and implementing procedural and technical standards for the deployment of network device security.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of the TrackVia SaaS. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business annually.

The following table details the procedures as they relate to the operation of the TrackVia SaaS:

Procedures	
Procedure	**Description**
Policy Management and Communication	Policies are maintained by the Director of Information Security and HR. All polices are available via the corporate shared drive. Employees are expected to review and adhere to all policies.
Operations Security	The Company has established procedures on the proper management of IT production, including change management, capacity management, malware, backup, logging, monitoring, installation, and vulnerabilities.
Network Operations	Communications security is governed by procedures that define controls related to network security, segregation, network services, transfer of information, and messaging.
Enterprise Change Management	Changes to the architecture and the configuration of servers is managed by Production Operations. Changes are required to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

Procedures	
Procedure	**Description**
Incident/Problem Management	The Company has established incident/problem management procedures, including reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence.
Backup and Offsite Storage	Daily incremental and daily full backups are carried out to ensure that the Company can recover from unforeseen events, system failure, or accidental or deliberate loss of information or facilities.
System Development	A software development life cycle (SDLC) is in place. A SDLC is a process followed for a software project that consists of a detailed plan describing how to develop, maintain, replace, and enhance software. The SDLC defines a methodology for improving the quality of software and the overall development process.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. The TrackVia SaaS is a hosted application platform. TrackVia provides customers with the ability to create custom models that match their data and workflow. Customers upload their data into these models and TrackVia becomes the source of record. The data that is uploaded into the system is chosen by the customer and is unique for each customer.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- User entities should have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities should only grant access to the Company's system to authorized and trained personnel.

- Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
- User entities should deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

AWS

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to the TrackVia SaaS cover only a portion of the overall internal control for each user entity of the TrackVia SaaS.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the TrackVia SaaS to be achieved solely by the Company. The CSOCs that are expected to be implemented at AWS are described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS encrypts databases in its control.
CC6.4	• AWS restricts data center access to authorized personnel. • AWS monitors data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS securely decommissions and physically destroys production assets in its control.
CC7.2 A1.2	• AWS installs fire suppression and detection and environmental monitoring systems at its data centers. • AWS protects data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS oversees the regular maintenance of environmental protections at its data centers.

Workato

The Company uses Workato as a subservice organization to power TrackVia Integration Services. TrackVia Integration Services is an optional TrackVia SaaS service component that provides a low-code approach to integration with external information systems. Workato's controls related to the TrackVia SaaS cover data that is processed by Workato en route to or from the TrackVia SaaS and a customer defined external system. Data passing through Workato is stored temporarily in transaction logs.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at Workato related to confidentiality, integrity, and availability of TrackVia customer data.

Company management receives and reviews the Workato SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by Workato to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at Workato, and relay any issues or concerns to Workato management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the TrackVia SaaS to be achieved solely by the Company. The CSOCs that are expected to be implemented at Workato are described below.

Criteria	Complementary Subservice Organization Controls
CC2.3	• Workato notifies customers of critical changes that may affect their processing. • Workato implements boundary protections to safeguard its production network.
CC4.1 CC4.2 CC7.1 CC7.2 CC7.3	• Workato monitors its systems for performance, capacity, security events, resource utilization, and unusual system activity.
CC6.1	• Workato encrypts data stores housing sensitive customer data.
CC6.7	• Workato uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
CC7.2 A1.1 A1.2 A1.3	• Workato designs and implements environmental protections, software, and data backup and recovery processes to meet its high availability objectives.
C1.2	• Workato purges or removes customer data containing confidential information from the system environment when customers leave the service.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Principal Service Commitments

Commitments are declarations made by management to customers regarding the performance of the TrackVia SaaS. Commitments are communicated in writing in a Master Services Agreement (MSA) and the General Terms and Conditions. The Company's principal service commitments include:

- Providing the hosted services with at least a 99.5% system availability.
- Not using confidential information for any purpose not expressly permitted by the MSA.
- Only disclosing confidential information to the employees or individual independent contractors that have a need to know such confidential information for the purposes expressed in the MSA and who are under a duty of confidentiality.
- Protecting confidential information from unauthorized use, access, or disclosure in the same manner that TrackVia protects its own confidential or proprietary information of a similar nature and with no less than a reasonable degree of care.
- Upon termination of the services, TrackVia will use commercially reasonable efforts to maintain customer data for 30 days.

Principal System Requirements

System requirements are specifications regarding how the TrackVia SaaS should function to meet the Company's commitments to user entities. System requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as user IDs and passwords to access systems
- Protection of data in transit and at rest
- Risk assessment and risk mitigation standards
- System monitoring
- Change management procedures
- Security requirements under the Health Insurance Portability and Accountability Act (HIPAA)