AARC 360

Assurance | Advisory
Risk | Compliance

PICARRO

Picarro, Inc.
Independent Service Auditor's Report SOC 3 at a Service Organization Relevant to Security

February 1, 2021 through January 31, 2022

www.AARC-360.com

PICARRO

Table of Contents

SECTION 1 – INDEPENDENT SERVICE AUDITOR'S REPORT

AARC-360

8000 Avalon Boulevard, Suite 100 Alpharetta, GA 30009

Tel: +1 866 576 4414

www.AARC-360.com

Assurance | Advisory
Risk | Compliance

Independent Service Auditor's Report

To: Picarro, Inc.

Scope

We have examined Picarro, Inc.'s ('Picarro', 'the Company', or 'the Service Organization') accompanying assertion titled "Assertion of Picarro, Inc. Management" (assertion) that the controls within Picarro's Natural Gas Solutions (system) were effective throughout the period February 1, 2021 through January 31, 2022, to provide reasonable assurance that Picarro's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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).*

Picarro uses a cloud hosting provider to provide a server and serverless data processing environment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Picarro, to achieve Picarro's service commitments and system requirements based on the applicable trust services criteria. The description presents Picarro's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Picarro's controls. The description does not disclose the actual controls at the cloud hosting provider. Our examination did not include the services provided by the cloud hosting provider, 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 Picarro, to achieve Picarro's service commitments and system requirements based on the applicable trust services criteria. The description presents Picarro's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Picarro'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

Picarro 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 Picarro's service commitments and system requirements were achieved. Picarro has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Picarro 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 Picarro'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 Picarro's service commitments and system requirements based 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 Picarro's Natural Gas Solutions were effective February 1, 2021 through January 31, 2022, to provide reasonable assurance that Picarro's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

AARC-360

Alpharetta, Georgia
June 2, 2022

PICARRO

SECTION 2 – ASSERTION OF PICARRO, INC. MANAGEMENT

PICARRO

Assertion of Picarro, Inc. Management

June 2, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Picarro, Inc. ('Picarro', 'the Company', or 'the Service Organization') Natural Gas Solutions (system) throughout the period February 1, 2021 through January 31, 2022, to provide reasonable assurance that Picarro's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

Picarro uses a cloud hosting provider to provide a server and serverless data processing environment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Picarro, to achieve Picarro's service commitments and system requirements based on the applicable trust services criteria. The description presents Picarro's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Picarro's controls. The description does not disclose the actual controls at the cloud hosting provider.

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

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2021 through January 31, 2022, to provide reasonable assurance that Picarro's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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)*. Picarro'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 4.

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, 2021 through January 31, 2022, to provide reasonable assurance that Picarro's service commitments and system requirements were achieved based on the applicable trust services criteria.

Patrick Pittier
DevOps Director
Picarro, Inc.

SECTION 3 – PICARRO, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS NATURAL GAS SOLUTIONS

Picarro, Inc.'s Description of Its Natural Gas Solutions throughout the period February 1, 2021 through January 31, 2022

Company Background

Picarro Inc. was founded in 1998 and is headquartered in Santa Clara, CA. Picarro's Natural Gas Solution is a combination of hardware, software, and data analytics. The vehicle mounted Picarro systems conduct multiple patrols through a natural gas infrastructure, collecting methane plume data and sending it to the Picarro cloud where analytics then transform the data into actionable results for a number of applications, from leak survey to pipe replacement to risk and emission reduction.
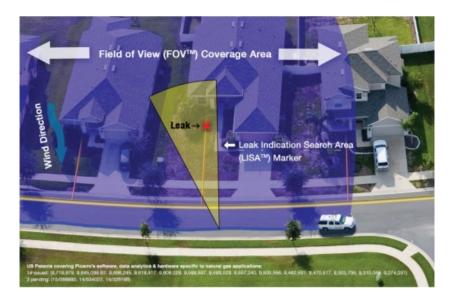
The Picarro system identifies the characteristic signatures of natural gas leaks by analyzing the methane plumes as they propagate in the atmosphere and intersect with the path of the vehicle. The system also measures atmospheric and meteorological conditions and uses algorithms to identify the origin and degree of hazard of the natural gas leak indication while virtually eliminating indications triggered by other non-natural gas sources of methane. A key feature of the Picarro system is its ability to combine information from multiple measurement sessions over a region, taking advantage of varying atmospheric conditions (wind direction, wind speed, atmospheric stability), to produce aggregated survey results over a certain period of time. This capability increases territory coverage with successive passes by the vehicle and allows statistics to be built up on location and risk for every leak indication. Reports and other data outputs can be generated from this processed data specific to the intended use case – leak survey, forecasting, targeted emissions reduction, risk management, etc.

Overview of Services Provided

The Picarro Solution is a multiuser, transaction-based application that enables the collection of data from field sensors and applies proprietary algorithms which generate real-time visualizations, aggregated reports and actionable insights. Key capabilities include:

- Capturing atmospheric data from gas utility networks and pipelines.
- Qualitive emissions indications.
- Visualization of leak data with customer GIS data.
- Providing data reporting in a variety of formats.

Picarro uses an Advanced Leak Detection concept that utilizes the wind to bring methane plumes to Picarro's vehicle-based methane and atmospheric sensing platform. Picarro's data collection methodology is based on the ability of the Picarro system to detect methane emissions hundreds of meters away from the vehicle when the methane emission point is upwind of the vehicle. The reach of Picarro's Field of View (FOV) coverage area is calculated at each point along the vehicle path to provide documented record of survey coverage. In this way, both mains and services can effectively be surveyed. If methane is detected, the system computes a Leak Indication search area marker whose location and footprint is determined by wind direction and variability. The search area markers indicate likely leak locations that require further investigation on foot to pinpoint each leak. This patented concept is shown in the figure below.

Picarro's Advanced Leak Detection (ALD) Technique

Infrastructure

The Picarro Solution runs within a third-party cloud hosting provider.

Customers login to the Picarro Solution web application to visualize captured sensor data and generate reports. The Picarro Solution incorporates a Single Sign-On (SSO) platform which provides options to integrate with a customer's own SSO solution or Picarro's authentication model. The visualizations and reports can incorporate customer provided GIS, served by GeoServer, which is then overlayed onto Bing Maps tiles. Additional customized dashboards can be designed and visualized via Kibana and ESRI technologies to provide actionable data insights to customers using the Picarro Solution.

Software

The Picarro Solution is developed by Picarro's in-house software engineering group. The software engineering group enhances and maintains the platform to provide service and features for its customers. Picarro's software is not sold on the open market.

The Picarro Solution tracks information in real time. The information is immediately stored in a database and is accessible for instant reporting. The information can be retrieved, reviewed, and reported as needed to help with Leak Survey, Risk Reduction & Emission Reduction purposes.

GIS customer data requires geoprocessing and data manipulation in order to be able to load and display in GeoServer. Customer data is provided through a secure file transfer protocol (SFTP). Visualization and geoprocessing of the spatial data is executed with ESRI software.

The Picarro Solution web interface is a multi-user, web-based application that enables multiple use cases including Leak Survey, Risk Reduction & Emission Reduction.

People

Picarro has a staff of approximately 220 employees organized in the following functional areas:

- *Corporate:* Executives, senior operations staff, and company administrative support staff, such as legal, marketing, sales, internal audit, training, accounting, finance, human resources, IT and Engineering.
- *Operations:* Staff that administers the production, testing and support of analyzers.
  - Integration and testing of the analyzer hardware and software components to ensure the system is operating within specifications.
    Service, support, maintenance and RMA processing of the analyzer software and hardware.
- *Software Engineering*: Software Development, QA, IT, DevOps and Security
  - The software development staff develops and maintains the custom software for Picarro. This includes the Picarro Solution, supporting utilities, and the external websites that interact with the platform.
  - The QA team performs both automated and manual quality testing of software changes before software is released to production.
  - The DevOps team manages the infrastructure and software releases into the production environment for the Picarro Solution.
  - The security staff supports the Picarro Solution indirectly by monitoring internal and external security threats and maintaining current antivirus software.
  - IT personnel maintain the voice communications environment, provide user support to Picarro, and resolve communication problems. This group does not directly use the platform, but it provides infrastructure support as well as disaster recovery assistance.
  - *Field Application Engineering (FAE)*: Support for the Picarro Solution field deployment, customer onboarding and training, preventive maintenance and customer service.
  - The FAE team provides direct customer support for use of the platform, field sensor end-user training and application use.

Data and Reporting

Data, as defined by Picarro, constitutes the following:

- Raw data
- Post-processed data
- GIS Data
- Survey data
- Output reports
- System files
- Error logs

The field sensors generate a raw data pipeline which is ingested into the platform and post-processed with Picarro's proprietary algorithms. Output reports are available in electronic PDF, comma-delimited value file exports, or directly viewable from the web interface. The access to review or download reports is based on the role defined for a user. Reports delivered externally will only be sent using a secure method—encrypted email, secure FTP, or secure websites over connections secured by trusted security certificates.

Processes and Procedures

Management has developed procedures to restrict logical access to the platform and communicated these procedures to Field Application Engineers, Operations and Engineering teams. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- 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, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

SECTION 4 – PICARRO'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Picarro, Inc.'s Principal Service Commitments and System Requirements

Picarro designs its processes and procedures related to Picarro to meet its objectives for its Natural Gas Solutions. Those objectives are based on the service commitments that Picarro makes to user entities, the laws and regulations that govern the provision of Natural Gas Solutions and the financial, operational, and compliance requirements that Picarro has established for the services. The Natural Gas Solutions of Picarro are subject to the security requirements in accordance with client contractual obligations.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Natural Gas Solutions that are designed 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
- Use of encryption technologies to protect customer data both at rest and in transit

Picarro establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Picarro'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. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Natural Gas Solutions.

Complementary Subservice Organization Controls (CSOCs)

Picarro utilizes a subservicing organization to perform certain key operating functions for the Natural Gas Solutions Services. The accompanying description of controls includes only those policies, procedures and controls at Picarro, and does not extend to policies, procedures and controls at the Subservice Organization.

Cloud Hosting Provider

Picarro uses a cloud hosting provider, or the 'Subservice Organization') to provide Infrastructure as a Service (IaaS) in support of its Natural Gas Solutions Services and the following table presents the applicable Trust Services Criteria that are intended to be met by controls at the subservice provider, alone or in combination with controls at Picarro, and the types of controls expected to be implemented at the subservice provider to meet those criteria.

The Picarro Natural Gas Solutions Services is built on top of the cloud hosting provider's IaaS product. The cloud hosting provider undergoes its own rigorous audit processes to include an annual AICPA based SOC 2 audit and is examined annually by Picarro. It is expected that the Subservice Organization has implemented the following types of controls to support the associated criteria.

Subservice Organization	Services Provided	Control
Cloud Hosting Provider	Data Center Hosting Services	Logical access control systems are utilized by the organization to control permissions and privileges to systems where Picarro data is stored.
		Physical security protections are in place for the organization's secure areas within the facility where Picarro systems/data is hosted.
		Only authorized personnel have access to create, alter, and revoke access badges where Picarro systems/data is hosted.
		A badge access control system exists in the facility to control physical access movement into and throughout the facility and that access is appropriate where Picarro systems/data is hosted.
		Access to the facility's onsite data center is restricted to authorized personnel where Picarro systems/data is hosted.
		The Subservice Organization is responsible for installation of the suppression and detection, and environmental monitoring systems at the data centers where Picarro data is stored. The Subservice Organization is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS) where Picarro data is stored. The Subservice Organization is responsible for overseeing the regular maintenance of environmental protections at data centers where Picarro data is stored.

Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary user entity controls considered in the design of Picarro's controls are suitably designed and operating effectively, along with related controls at Picarro. Complementary User Entity Controls are specific user controls or issues each Picarro client organization should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by user entities, nor do they represent procedures that may be necessary in all circumstances.

1. User entities and subservice organizations are responsible for understanding and complying with their contractual obligations to Picarro.
2. User entities are responsible for notifying Picarro of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Picarro's services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Picarro's services.
6. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
7. User entities are responsible for ensuring that data submitted to Picarro is complete, accurate, and timely.
8. Standards and processes are in place for user entities to follow for security and industry guidelines.