



SOC 3® Report

Controls Relevant to Security, Availability, and Confidentiality

For the Period July 1, 2022 to June 30, 2023

Prepared in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA)



Table of Contents

Independent Service Auditor's Report	1
Assertion of Plivo Inc Management	3
Management's System Disclosures	4
Types of Services Provided	4
Boundaries of the Platform	4
Principal Service Commitments and System Requirements	11



Independent Service Auditor's Report

To the Management of Plivo Inc
Austin, Texas

Scope

We have examined Plivo Inc's (the Company) accompanying assertion titled "Assertion of Plivo Inc's Management" (assertion) that the controls within the Plivo Cloud Communication Platform (the Platform) were effective throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that the Company'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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the Platform to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled "Assertion of Plivo Inc Management" about the effectiveness of controls within the Platform. When preparing its assertion, the Company 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 Platform.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that the controls within the Platform were effective throughout the period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted following attestation standards established by the 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 the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent of the Company and to meet our other responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

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

There are inherent limitations in 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 suitability of the design or 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.

Opinion

In our opinion, management's assertion that the controls within the Platform were effective throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

MJD Advisors

Waukee, Iowa
August 5, 2023



Assertion of Plivo Inc Management

We, as management of Plivo Inc, are responsible for designing, implementing, operating, and maintaining effective controls within the Platform throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that the Company's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. We have described the boundaries of the Platform in the section titled "Management's System Disclosures" (the System Disclosures), which identifies the aspects of the Platform covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the Platform throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that the Company'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*).

The Company's objectives for the Platform 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 the System Disclosures.

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 Platform were effective throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria.

Management of Plivo Inc
August 5, 2023

Management’s System Disclosures

Types of Services Provided

The Plivo Cloud Communication Platform is a Communications Platform as a Service (CPaaS) offering that provides a real-time, cloud-based, customized communication service integrated with existing web and mobile applications. Customers leverage the Platform’s APIs for various communication use cases, including voice calling, call forwarding, voice, and SMS & MMS notifications, two-factor authentication, and one-time passwords. The Platform also offers carrier management, call quality, message deliverability, and 24/7 emergency technical support.

The system description that follows is specific to the Company’s cloud communications services. Other separate service offerings provided by Plivo Inc, such as Sellular, which offers an omnichannel sales engagement platform, and Contacto, which is a cloud contact center solution, are not within the scope of this system description.

Boundaries of the Platform

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle, such as initiation, authorization, processing, recording, and reporting for the services provided to user entities. The system boundaries do not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

Infrastructure

The Company leverages the experience and resources of Amazon Web Services (AWS) to provide the primary resources for the Platform’s infrastructure and utilizes Redis Labs to manage its in-memory data store. However, the Company is responsible for designing and configuring the Platform architecture within the cloud hosting environment to ensure security and resiliency requirements are met. The specific resources leveraged from AWS include the following:

Cloud Hosting Services	
Service	Description
AWS ECS	Managed container service
Amazon ECR	Managed container registry
Amazon RDS	Managed relational database service
Amazon Elastic Compute Cloud	Compute service
AWS S3	Object storage
AWS Lambda	Serverless, event-driven, compute service

Cloud Hosting Services	
Service	Description
Amazon Redshift	Managed data warehouse service
Amazon OpenSearch Service	Distributed search and analytics engine
Amazon Elastic File System	Shared file storage system
Amazon ElastiCache	Managed caching service
Amazon Kinesis	Processes streaming data
Application Load Balancer	Managed load balancing service
Amazon Route 53	Domain Name System
Amazon CloudFront	Content delivery network
AWS CloudTrail	Infrastructure activity monitoring
Amazon CloudWatch	Infrastructure resource and application monitoring
Amazon GuardDuty	Threat detection service
Amazon Inspector	Security assessment and vulnerability management service
AWS Certificate Manager	Manages public and private SSL/TLS certificates
AWS KMS	Cryptographic key management
AWS WAF	Web application firewall
Amazon API Gateway	Managed API service
AWS Secrets Manager	Manages API keys, OAuth tokens, and other secrets
AWS Config	Monitors, records, and evaluates AWS resource configurations
AWS Systems Manager	Operations hub for AWS infrastructure
AWS Virtual Private Cloud	Provides a logically isolated virtual network that uses network security groups to control traffic

Certain controls of AWS are necessary in combination with the Company's controls to provide reasonable assurance that the Company's service commitments and system requirements are achieved based on the trust services criteria (Complementary Controls). The Company is responsible for the oversight and monitoring of AWS, which is performed through the vendor management policies and procedures.

The following are the applicable trust services criteria and controls that are necessary to be in place at AWS to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

Complementary Controls	
Criteria	Control
Logical and Physical Access CC6 Series	<p>Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts and procedures are implemented to decommission and physically destroy production assets securely.</p> <p>Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by the Company, to secure the transmission and storage of information.</p>
System Operations CC7 Series	<p>Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities.</p> <p>Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.</p>
Change Management CC8 Series	<p>Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.</p>
Availability A Series	<p>Monitoring tools are implemented to monitor and manage the capacity and availability of hosting infrastructure.</p> <p>Environmental protections, data backup processes, and recovery mechanisms have been implemented and appropriately tested to adequately address availability requirements.</p>

The examination performed by the independent service auditor did not extend to the policies, procedures, and controls of AWS.

Software

Software consists of the programs and software that support the Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Platform includes the following:

Software Summary	
Application	Purpose
Tugboat Logic	Compliance management platform
Sensu, Kibana, Grafana	Application monitoring
HCP Packer	Automates build configuration
Jenkins	CI/CD
Statuspage	Status and incident communication
Jira	Project management and issue tracking
Apple and Google	Push notification and cloud messaging services
Manage Engine, Kandji, Crowdstrike	Mobile device management, antivirus prevention, endpoint threat detection, and continuous zero trust checks
Google Workspace	File storage, email, document collaboration, identity provider
GitHub	Source code repository
Slack	Communication hub
Salesforce, Hubspot	Customer relationship management
OpsGenie	Centralized alerts and notifications
Akamai	Web application firewall and CDN
Trivy	Container scanning
AWS VPN	Virtual Private Network (VPN) with Multi-Factor Authentication Enabled
ClamAV	Antivirus engine for detecting viruses, malware, and other threats
SonarQube	Self-managed, automatic code review tool

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. The table below summarizes the key roles and functional responsibilities of the Company. Due to the Company's size, one individual may serve multiple roles.

Organizational Structure	
Role	Function
Executive Management	Responsible for oversight, implementation and continual improvement of the Information Security Program and includes the CTO and leaders from Legal, Security, and PeopleOps
CEO	Responsible for oversight of the development and performance of internal controls and for the direction of company-wide activities delegated to Executive Management
CTO	Responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Security Team	Responsible for the development, testing, deployment, and maintenance of the Platform and maintaining security and includes multiple functional teams, including Engineering, DevOps, Information Technology, and Network and Security Operations
Engineering	Responsible for the development, testing, deployment, and maintenance of the Platform and for maintaining security
Sales, Customer Support, and Success	Responsible for the development of new business, onboarding of customers, and technical support
Legal	Responsible for compliance and legal functions of the Company, including external attorneys providing services under management supervision
Product	Responsible for guiding the overall direction of the product roadmap, including usability, enhancements, and new features
PeopleOps	Responsible for managing the onboarding, performance management, and personnel termination processes

Procedures

Procedures are the specific actions undertaken to implement a process, consisting of linked procedures designed to accomplish a particular goal. Policies, which serve as the basis of procedures, are management's statements of what should be done to meet system objectives and may be documented, explicitly stated in communications, or implied through actions and decisions.

The Company has adopted the following defined set of information security standards and policies (described as the Information Security Program throughout the report):

- | | |
|--|---|
| 1. Acceptable Use Policy | 2. Incident Management Policy |
| 3. Access Control Policy | 4. Information Classification Policy |
| 5. Asset Management Policy | 6. Information Security Policy |
| 7. Backup and Restoration Policy | 8. IT and Communications Systems Policy |
| 9. Change Management Policy | 10. Key Management and Cryptography Policy |
| 11. Clean Desk and Clear Screen Policy | 12. Mobile Device Management Policy |
| 13. Code of Business Conduct & Ethics | 14. Network Security Policy |
| 15. Confidential Communication Policy | 16. Personnel Security Policy |
| 17. Customer Support and SLA Policy | 18. Physical and Environmental Security Policy |
| 19. Data Integrity Policy | 20. Risk Assessment Policy |
| 21. Data Retention and Disposal Policy | 22. Server Security Policy |
| 23. Disciplinary Policy | 24. Serverless Security Policy |
| 25. Uses and Disclosures of PHI Policy | 26. Software Development Policy |
| 27. Breach Notification Policy | 28. Vendor Management Policy |
| 29. Internal Privacy Policy | 30. Vulnerability Management Policy |
| 31. Internal Audit Policy | 32. Workstation Security Policy |
| 33. Business Continuity and Disaster Recovery Policy | 34. Technology Equipment Handling and Disposal Policy |
| 35. Password Policy | 36. Threat Intelligence Policy |
| 37. Data Loss Prevention (DLP) Policy | 38. Data Masking Policy |
| 39. Logging and Monitoring Policy | 40. Social Engineering Awareness Policy |

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners. The following table details the types of data collected by the Company in connection with the Platform's services and the infrastructure, software, and third-party vendors utilized to store and process the data.

Data Type Summary		
Type	Description	Storage and Processing
Account data	Personally Identifiable Information and other administrative data from personnel, customers, and other third parties	AWS and certain 3rd party SaaS tools subject to the vendor management process
Communication services	Voice recordings, telephone numbers, call log metadata, text messages	AWS
Internal Log Information	Information relevant to and explicitly necessary for services, including metadata	Kibana, Amazon CloudWatch, AWS CloudTrail
PHI	Information obtained from Covered Entities and Business Associates that is processed according to Business Associates Agreements (BAAs) and protected under the requirements of HIPAA	AWS provides data processing services for PHI and is engaged with a BAA. Amazon RDS and AWS S3 are utilized to store PHI
Secrets	Access credentials, tokens, certificates, API keys, and other secrets	AWS Secrets Manager

Principal Service Commitments and System Requirements

The information presented within the Boundaries of the Platform was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

Service Commitments

Service commitments include those made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security objectives and commitments are made available to customers through BAAs, Managed Services Agreements, and information shared on the Company's website, including a dedicated security page. The following summarizes the Company's principal service commitments that management believes to be relevant to the report users:

- The Company uses commercially reasonable physical, managerial, and technical safeguards designed to secure data from accidental loss and unauthorized access, use, alteration, and disclosure and maintains compliance with the requirements of HIPAA.
- Plivo provides logical tenant separation, encryption in transit (TLS 1.2 or greater), and encryption at rest utilizing AES-256.
- Phone number verification is delivered through an SMS text message or a voice call to the user's phone to activate new accounts, and unique Authentication IDs and tokens are used for every user.
- The Company logs all external and internal access to customer data.
- The Company leverages a mobile device management solution to monitor, manage, update, and secure personnel laptops and workstations and has the ability to remotely wipe devices.
- The Company responds to priority one business-critical incidents 24/7 and utilizes third-party notifications and alert systems to identify and manage threats.
- The Platform utilizes fault-tolerant network support and provides a 99.99% uptime SLA.
- The Company performs daily, automatic backups of all customer and system data to a different availability zone in the same region.

System Requirements

The Company's system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop services provided.