SOC 3® Report

Controls Relevant to Security, Availability, and Confidentiality

For the period April 1, 2022 to June 30, 2022

Prepared in Accordance with Attestation Standards Established by the AICPA

Table of Contents

Section 1: Independent Service Auditor's Report

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. Management" (assertion) that the controls within the Company's Plivo Cloud Communication Platform were effective throughout the period April 1, 2022 to June 30, 2022, 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* (trust services criteria).

The Company uses a subservice organization to provide cloud hosting services. The disclosures in Section 3 indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable criteria. The disclosures in Section 3 do 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 disclosures in Section 3 indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable criteria. 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

The Company 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 the Company's service commitments and system requirements were achieved. The Company has also provided the accompanying assertion about the effectiveness of controls within the system. 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 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 the Company'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 the Company'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 and we are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 Company's Plivo Cloud Communication Platform were effective throughout the period April 1, 2022 to June 30, 2022, 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
September 3, 2022

Section 2: Management's Assertion

Assertion of Plivo, Inc. Management

We, as management of Plivo, Inc. (the Company), are responsible for designing, implementing, operating, and maintaining effective controls within the Company's Plivo Cloud Communication Platform (the Platform) throughout the period April 1, 2022 to June 30, 2022, to provide reasonable assurance that the Company's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our disclosure of the boundaries of the Platform is presented in Section 3 and 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 April 1, 2022 to June 30, 2022, 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, 2*017 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 Section 3.

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 April 1, 2022 to June 30, 2022, 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.
September 3, 2022

Section 3: Management's System Disclosures

Management's System Disclosures for the Plivo Cloud Communication Platform

Types of Services Provided

The Plivo Cloud Communication Platform (the 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 API's 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.

Principal Service Commitments and System Requirements

The disclosures pertaining to the Platform were prepared to describe the procedures and controls the Company has 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 is meant to enable 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 security, availability, and confidentiality. The Company primarily communicates its service commitments to user entities through Managed Services Agreements and a security page made available on its public website. The following summarizes the Company's principal service commitments that management believes to be relevant to the report users:

- Customer data is encrypted at rest and access is limited based on the principle of least privilege.
- Content is transferred over end-to-end encryption using TLS 1.2 at every point of transfer.
- 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 1 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.

Boundaries of the Platform

Infrastructure

The Company leverages the experience and resources of Amazon Web Services (AWS) to scale quickly and securely as necessary to meet current and future demand. 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 - AWS	
Service	**Description**
AWS ECS	Managed container service
Amazon ECR	Managed Docker container registry
Amazon RDS	Managed relational database service
AWS S3	Object Storage
AWS Lambda	Serverless, event-driven, compute service
Amazon RedShift	Cloud data warehouse
Amazon OpenSearch Service	Managed Elasticsearch service
Amazon Elastic File System	Serverless, elastic, file system
Amazon ElastiCache	Managed caching service
Amazon Kinesis	Data streaming service
AWS Elastic Load Balancing	Distributes network traffic across available resources
Amazon Virtual Private Cloud	Provides a logically isolated virtual network for the production environment and controls traffic via security groups
Amazon Route 53	Domain name system
Amazon CloudFront	Content delivery network
AWS CloudTrail	Monitors and records user activity across AWS infrastructure
Amazon CloudWatch	Collects logs and presents metrics for monitoring AWS infrastructure
Amazon GuardDuty	Threat detection service
Amazon Inspector	Automated security assessment service
AWS Certificate Manager	Manages public and private SSL/TLS X.509 certificates and keys
AWS Key Management Service	Manages cryptographic keys and provides access controls
AWS WAF	Web application firewall
Amazon API Gateway	Managed service for developing, managing, and securing APIs
AWS Secrets Manager	Manages database credentials, API keys, and other secrets

Management has deemed the cloud hosting services provided by AWS meet the definition of a subservice organization. As such, complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements. The following are the applicable trust services criteria and controls that are necessary to be in place at the subservice organization to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

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

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 include 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	System status monitoring and notification service
Jira	Issue tracking and project management
Redis Labs	Caching provider
Apple and Google	Push notification and cloud messaging services
ManageEngine, Kanji, CrowdStrike	Mobile device management, antivirus prevention, and endpoint monitoring
Google Workspace	File storage, email, document collaboration, single sign on, MFA
GitHub	Source code repository
OpsGenie	Centralized alert management
Akamai	Content delivery, WAF
Trivy	Vulnerability and misconfiguration scanning

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. The below table summarizes the key roles and functional responsibilities for 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 overseeing company-wide activities, establishing and accomplishing goals, managing objectives and oversight of the performance of internal control.
CTO	Responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program.

Organizational Structure	
Role	**Function**
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 development of applications and services and implementation of security practices.
Sales, Customer Success, Customer Support	Responsible for the development of new business, onboarding of customers, and technical support.
Legal	Responsible for compliance and legal function of the Company and includes external attorneys providing services under the supervision of management.
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.

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, or 3rd party vendors utilized to store and process the data.

Data Type Summary		
Type	**Description**	**Storage and Processing**
Personally Identifiable Information	Data from personnel, customers, users, and other third parties such as suppliers, vendors, and business partners.	AWS infrastructure and other services described in Software
PHI	Information obtained from Covered Entities and Business Associates that is processed according to BAAs and protected under the requirements of HIPAA.	Amazon RDS and AWS S3 are utilized to store PHI and AWS is engaged with a BAA
Internal log information	Information that is relevant to and explicitly necessary for services, including metadata.	Kibana, Amazon CloudWatch, AWS CloudTrail
Communication Services	Voice recordings, telephone numbers, call log metadata, text messages.	AWS infrastructure
Secrets	Credentials, API keys, and OAuth tokens.	AWS Secrets Manager

Relevant Policies and Procedures

Procedures are the specific actions undertaken to implement a process, consisting of a series of linked procedures designed to accomplish a particular goal. Policies, which serve 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):

- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Backup and Restoration Policy
- Change Management Policy
- Clean Desk and Clear Screen Policy
- Code of Business Conduct & Ethics
- Confidential Communication Policy
- Customer Support and SLA Policy
- Data Integrity Policy
- Data Retention and Disposal Policy
- Disciplinary Policy
- Uses and Disclosures of PHI Policy
- Breach Notification Policy
- Internal Privacy Policy
- Internal Audit Policy
- Business Continuity and Disaster Recovery Policy
- Incident Management Policy
- Information Classification Policy
- Information Security Policy
- IT and Communications Systems Policy
- Key Management and Cryptography Policy
- Mobile Device Management Policy
- Network Security Policy
- Personnel Security Policy
- Physical and Environmental Security Policy
- Risk Assessment Policy
- Server Security Policy
- Serverless Security Policy
- Software Development Policy
- Vendor Management Policy
- Vulnerability Management Policy
- Workstation Security Policy
- Technology Equipment Handling and Disposal Policy

Control Environment

The Company's control environment describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. Executive Management is responsible for the oversight of the Information Security Program as defined in the Executive Management Charter. These responsibilities are carried out through the Company's organizational structure with expectations for integrity and ethical values which are described in the Company's Code of Business Conduct & Ethics.

Communication and Information

A critical objective for the Company is ensuring relevant, quality information is obtained or generated to support the functioning of internal control. The Information Security Program is made available to all personnel in a shared workspace and personnel are required to review and acknowledge its requirements upon hire and following any significant changes. Management also reinforces the Information Security Program in meetings, internal communication, and annual security training and awareness programs.

Risk Assessment

The Company has a defined risk management framework that is described in the Risk Assessment Policy and includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks. Risk assessments are performed at least annually and as part of that process, threats and changes (environmental, regulatory, and technological) to assets and service commitments are identified and the risks are formally assessed.

The first step of the risk assessment process is to identify assets within the scope of the Information Security Program. The objectives identified by management are specified in the risk management program to identify and assess risk related to the objectives. The Company's risk management processes include technical and nontechnical evaluation, such as penetration testing, vulnerability scanning and risk assessments, performed at an established cadence and in response to environmental or operational changes, to establish the extent to which the Platform is designed and controls are operating effectively to meet service commitments.

Monitoring Activities

The Company selects, develops, and performs ongoing and, if necessary, separate evaluations to ascertain whether the components of internal control are present and functioning. Management considers the rate of change in business and business processes when selecting and developing separate ongoing evaluations and utilizes the current state of the internal controls to establish a baseline.

The results of ongoing and separate evaluations are provided to the appropriate individuals to assess results. The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action and provide visibility to the CTO regarding the timeliness of remediation.

Control Activities

As part of its annual risk assessment, management selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Specifically, management selects and develops control activities designed and implemented to restrict technology access rights and achieve management's objectives over the acquisition, development, and maintenance of technology and infrastructure.

The Company has implemented control activities specific to the protection of confidential information throughout its lifecycle, including collection, processing and disposal which are described in the Information Classification Policy, Data Retention and Disposal Policy and Data Integrity Policy (the Data Management Policies). The Data Management Policies have been established to define the Company's data classification practices in accordance with legal requirements, sensitivity, and business criticality to ensure information is classified, protected, retained and securely disposed of in accordance with its importance. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Logical and Physical Access Controls

The Company has an established Access Control Policy that implements procedures for limiting access to individuals, software programs and infrastructure services that have been granted access rights. Duties and access to sensitive resources are established based on the principle of least privilege. Logical access to systems is restricted through the use of access control software and rule sets and is controlled by limited administrative users. The Company has established a formal onboarding and termination process and appropriate management approval is obtained prior to granting access to sensitive information.

Infrastructure supporting the service is monitored for malware by the Company and AWS through a shared responsibility model. The Infrastructure resources are built from the Center for Internet Security, Inc. (CIS) Hardened Container Images which are stored and managed in a private container registry and subject to scanning by Trivy and Amazon ECR.

System Operations

The Company has established baseline configuration standards for production servers and uses tools to detect and restore server configuration deviations from the standards. Infrastructure is monitored for noncompliance with the configuration standards, which could threaten the achievement of the Company's objectives. Certain third-party tools and procedures are used to identify potential vulnerabilities and deficiencies. Identified security deficiencies are tracked and prioritized through internal tools according to their severity.

The Company has an established Incident Management SOC Procedure that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents. Security events are quantified, monitored, and tracked by an identified incident response team, and procedures specified include collecting and preserving information that can serve as evidence. Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals. Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned. The Incident Management SOC Procedure requires creating, prioritizing, assigning, and tracking follow-ups to completion.

The Platform is hosted in multiple availability zones which are designed to fail independently, thus allowing the Platform to remain available when any single availability zone fails. Business and system recovery plans are documented, which provide the roles and responsibilities and detailed procedures for recovery of systems. Backups are configured to run automatically and production data is replicated in different availability zones. The integrity and completeness of backup information is tested on an annual basis. Processing capacity and usage are monitored on an automatic, real-time basis in order to appropriately manage capacity demand and load balancers are used to automatically distribute incoming application traffic across multiple instances and availability zones.

Business and system recovery plans are documented, which provide the roles and responsibilities and detailed procedures for recovery of systems. The Company has designed and configured the Platform for high availability and redundancy. The Platform's services are hosted utilizing multi-region active-active or active-passive recovery strategies. Backups of production data are performed according to the Data Management Policies and subject to similar security controls, including encryption methods, as the production data.

Change Management

The Company has an established Software Development Policy to ensure that information security and confidentiality are designed and implemented within the development lifecycle for applications and information systems. The change management processes and procedures have been established to plan, schedule, apply, distribute, and track changes to the production environment to minimize risk and client impact.

Risk Mitigation

The Company implements risk mitigation strategies to prioritize, evaluate and implement the appropriate risk-reducing controls recommended from the risk management process. The Company has established a formal Business Impact Analysis process to assess system criticality and data to drive business continuity requirements.

Management has identified potential business disruptions as a critical risk to meeting its objectives and has an established Business Continuity and Disaster Recovery Policy and Incident Management Policy to respond to, mitigate, and recover from security events that could disrupt business operations. Incident management policies and procedures are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from disasters, security events, and incidents.

As part of its risk mitigation strategies, management assesses and manages risks associated with vendors and business partners. Periodically, generally annually but performed relative to risk and changes in the environment, management assesses the risks that vendors and business partners represent to the achievement of the Company's objectives. As a general practice, the Company utilizes software and infrastructure resources and applications that are industry leaders and generally accepted amongst the security community.

Complementary User Entity Controls

The Company's services are designed with the assumption that certain controls will be implemented by user entities (or more specifically - its customers) and such controls are known as complementary user entity controls. It is not feasible for all of the trust services criteria related to the Company's services to be solely achieved by the Company's control procedures. Accordingly, user entities should establish their own internal controls or procedures to complement those of the Platform. The complementary user entity controls should not be regarded as a comprehensive list of all controls that user entities should implement. Management of user entities is responsible for the following:

- Ensuring the confidentiality of user accounts, Auth ID, Auth Tokens, and passwords.
- Implementing the Plivo Security Best Practices described on the Company's website.
- Notifying the Company promptly when changes are made to technical, billing, or administrative contact information.
- Developing internal disaster recovery and business continuity plans and breach notification procedures that address the inability to access or utilize the Company's services.
- Notifying the Company and providing accurate information regarding new, terminated and changes necessary to user accounts.
- Informing the Company of any regulatory issues that may affect the services provided.
- Understanding and complying with contractual obligations to the Company.
- Immediately notifying the Company of any actual or suspected information security breaches involving the Platform, including compromised user accounts.
- Granting access only to authorized and trained personnel.
- Deploying physical security and environmental controls for all devices and access points.