preset™

SOC 3 Report

Preset, Inc.

March 1, 2023 to May 30, 2023

An Independent Service Auditor's Report on Controls Relevant to Security

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

SECTION 1

Management's Assertion

preset

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Preset, Inc.'s system throughout the period March 1, 2023, to May 30, 2023, to provide reasonable assurance that Preset, Inc.'s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Attachment A [A] and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period March 1, 2023, to May 30, 2023, to provide reasonable assurance thatPreset, Inc.'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. Preset, Inc.'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 A [A].

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.

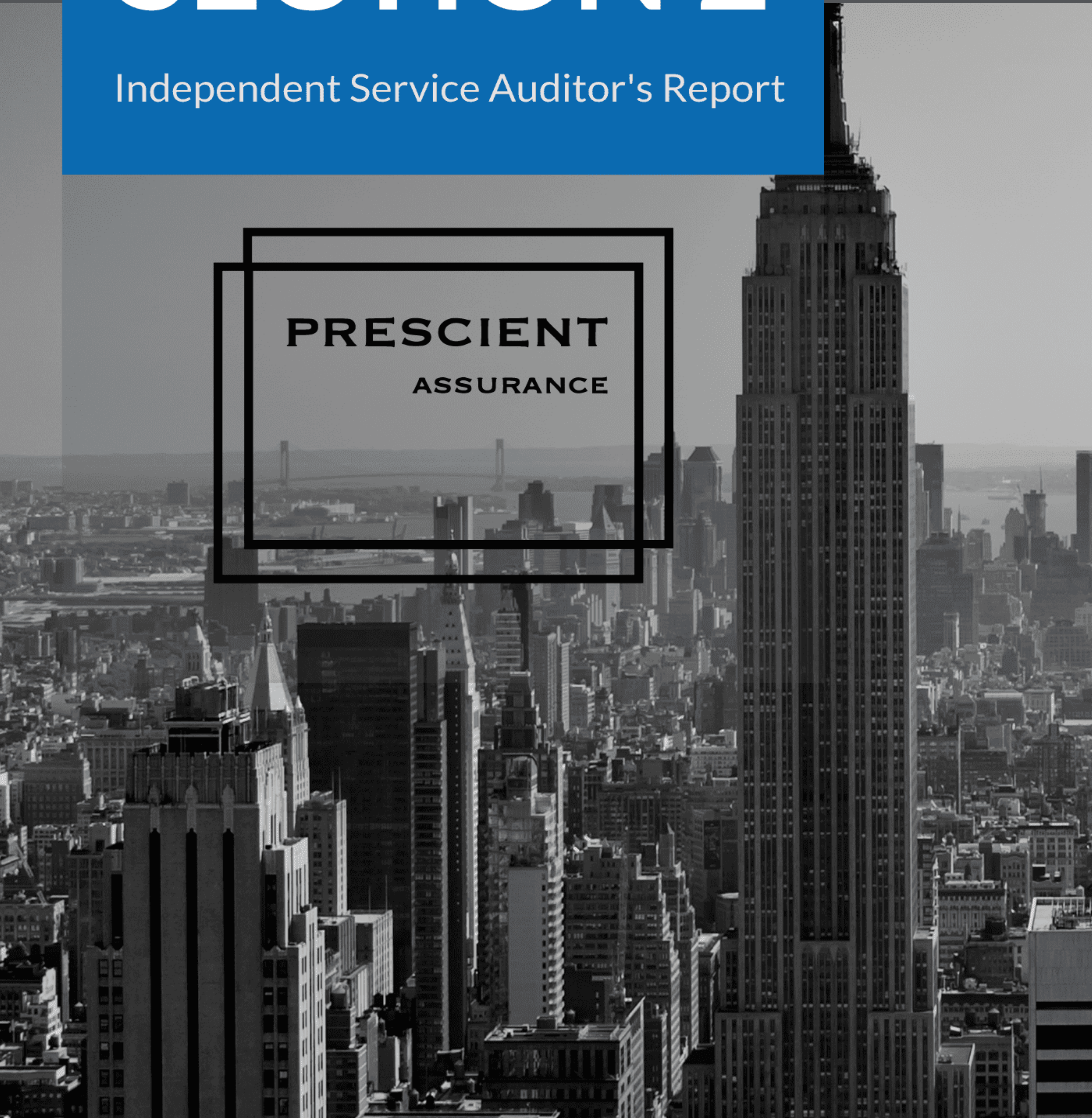
We assert that the controls within the system were effective throughout the period March 1, 2023, to May 30, 2023, to provide reasonable assurance that Preset, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
Maxime Beauchemin
C5EB896803A54D4...

Maxime Beauchemin
Founder and CEO
Preset, Inc.

SECTION 2

Independent Service Auditor's Report



PRESCIENT

ASSURANCE

Independent Service Auditor's Report

To: Preset, Inc.

Scope

We have examined Preset, Inc.'s accompanying assertion in Section I, titled "Management's Assertion" (the assertion) that the controls within Preset, Inc.'s system (the system) were effective throughout the period March 1, 2023, to May 30, 2023, to provide reasonable assurance that Preset, Inc.'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).

Service Organization's Responsibilities

Preset, Inc. 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 Preset, Inc.'s service commitments and system requirements were achieved. In Section I, Preset, Inc. has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Preset, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services 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

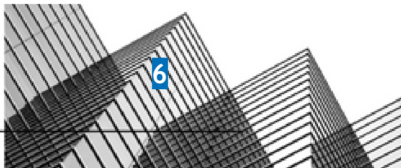
Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the 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 that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve Preset, Inc.'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 Preset, Inc.'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 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 risks 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 Preset, Inc.'s system were effective throughout the period March 1, 2023, to May 30, 2023, to provide reasonable assurance that Preset, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

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

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
January 9, 2024

SECTION 3

Attachment A

preset

DC 1: Company Overview and Types of Products and Services Provided

Apache Superset™ creator Maxime Beauchemin founded Preset in 2019 to make the power of Superset available to the widest possible audience as a SaaS offering. A leader in the open-source community, Max is the creator of Apache Airflow, an open-source tool for orchestrating complex computational workflows and data processing pipelines, and Apache Superset, the popular open-source project underpinning Preset. Superset grew quickly, taking on more and more use cases, eventually surpassing Tableau as Airbnb's main data visualization solution. Superset was established as a full-fledged open-source project, incubating with the Apache Software Foundation, in 2016. Today Superset is the leading open-source analytics platform, with one of the fastest-growing communities on GitHub and enterprise users at data-hungry companies like Airbnb, Lyft, and Twitter. Preset is combining the power of Superset with the agility of SaaS to enable businesses to quickly realize the power of data democratization within their organizations.

Through Preset, we're committed to doing the hard work needed to help Superset reach its full potential. That means investing in education, training, and documentation. It also means actively supporting the community by hosting meetups and conferences, answering questions, and managing releases. We'll take these steps and more in service of the big picture: making sophisticated data analysis and insights available to all by providing the right tool for the right person.

Preset is an open analytics data platform built on Apache Superset™, that makes teams productive with data.

With an intuitive visual interface, Preset empowers users to explore and analyze their data. Flexible dashboarding capabilities and a deep set of visualization types make communicating and sharing data-driven insights simple and fast. Lightweight and cloud-native, Preset supports the workflows of modern teams.

Preset features:

- An intuitive interface to explore and visualize datasets and create interactive dashboards
- A wide array of beautiful visualizations to showcase customer data
- Easy, code-free user flows to drill down and slice and dice the data underlying exposed dashboards. The dashboards and charts act as a starting point for deeper analysis
- A state-of-the-art Structured Query Language ('SQL') editor/integrated development environment ('IDE') exposing a rich metadata browser and an easy workflow to create visualizations out of any result set
- Enterprise-grade security and access controls that secure mission-critical customer data A lightweight semantic layer, allowing control over how data sources are exposed to the user by defining dimensions and metrics
- Out of the box support for most SQL-speaking databases

DC 2: The Principal Service Commitments and System Requirements

Preset's processes and procedures are based on service commitments that Preset makes to its customers as well as the financial, operational, legal, and compliance requirements that govern Preset business operations.

Preset has a description of their service offerings online. Security commitments are standardized and include, but are not limited to, the following:

- Preset restricts access according to job or customer role by design within their production service. Access is based on the rule of least privilege
- Preset operates under the principle of "encrypt everywhere" to protect company and customer data in transit, and at rest as required

Preset establishes and makes available to its employees through the Company Intranet the operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Preset'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 Preset service.

DC 3: The Components of the System Used to Provide the Services

People

Preset currently has a staff of approximately 30 employees organized in the following functional areas:

- Executive Team: Includes the Chief Executive Officer (CEO), VP Operations, VP Engineering, VP Sales, Head of Marketing, and Director of Customer Success.

Operations: Company administrative support staff that manages day-to-day functions in the following areas:

- People Team (Human Resources, Compensation, Recruiting)
- Office Management, Finance, Accounting, Legal
- Product Management, Product Design: Product manager, Designers and User Researchers
- Engineering: Frontend and Backend Software Engineers, DevOps, Infrastructure, Automation, Engineering Managers
- Product Marketing: Inbound/Outbound Marketing Staff, Product Marketing, Content Marketing, Community Managers, Developer Relations
- Customer Engagement: Customer relationship team; development of customer self-serve documentation and training, Solutions Engineers, Technical Support Engineers, Customer

Support Specialists, Customer Success Managers

Security Processes and Procedures

Presets Information security organization is led by the Director of Engineering and comprises the security team as well as the compliance team. The Security Organization is responsible for developing and distributing policies and procedures related to information and security standards, as well as compliance standards to Preset personnel. Policies and procedures are published on Preset's intranet. These policies and procedures are reviewed and updated on a periodic basis.

Third Party Access

Corporate name	Corporate location	Function
Aha	United States	Roadmap Planning
Atlassian	United States	Customer and User Support
Attivo	United States	Financial Services
Auth0	United States	Authentication Provider
Amazon Web Services	United States	Cloud Provider
Bytecode	United States	Professional Services for Specific Add-on Offerings
Chameleon	United States	Customer and User Support
Datadog	United States	Monitoring Service Provider
Google	United States	Workplace Productivity Tools
Google Cloud Platform	United States	Cloud Provider
HubSpot	United States	Marketing Platform
Mixpanel	United States	Usage Analytics
Okta	United States	Single Sign On Provider
Recurly	United States	Billing and subscription management

Corporate name	Corporate location	Function
Segment	United States	Data Pipeline
Sentry	United States	Log Analysis
Service Rocket	United States	Customer and User Support
Slack	United States	Workplace Productivity Tool
Sparkpost	United States	Email Service Provider
Threat Stack	United States	Intrusion Detection Service

System Boundaries

The scope of this report includes the Preset Cloud Data Analytics and Visualization Platform Services System performed in the San Mateo, California facility.

This report does not include the cloud hosting services provided by AWS at their multiple facilities.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

Integrity and Ethical Values

Integrity and ethical behavior are the product of Preset's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual

- The HR policy stipulates that a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties be signed by the employee
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

The skills and competence of employees and contractors are assessed by human resources staff and the hiring manager or his or her designees as part of the hiring process. Required skills and competencies are listed in job descriptions and requisitions. Competency evaluations may include reference checks, education and certification verifications, technical testing, and interviews.

Preset employees undergo an annual performance review which includes an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.

Preset employees and third parties with administrative or privileged technical access to Preset production systems and networks are made aware of relevant information security policies and procedures and must complete security awareness training at the time of hire and annually thereafter. Management monitors training completion and takes appropriate steps to ensure training is completed.

Employees are encouraged to continue their professional development through training, seminars, classes, certification, and industry events.

Management's Philosophy and Operating Style

Preset's management philosophy is based on Preset's core values:

- Be transparent - We share, include, and communicate with each other openly. We build trust through authenticity and clear intentions.
- Cultivate empathy - We seek to understand diverse thoughts, listen intently, communicate respectfully, and find informed solutions – with our coworkers, community, and customers.
- Be innovative - We creatively solve problems in unbounded ways. We challenge assumptions and value different points of view.
- Get it done - We drive impact, for our customers and for ourselves. We seek results, execute with purpose and own our work.

The operating style is built around the principles of service-oriented leadership, meritocracy of ideas, and agile development principles. Preset management is continually engaged with team members to identify and address issues that may impact employee satisfaction and performance. All team members are given the opportunity to present their ideas and we collectively work together to translate those ideas into products and services. Preset follows agile development processes to ensure adequate planning, risk management, and robust feedback loops lead to quality products and services that delight our customers.

Organizational Structure and Assignment of Authority and Responsibility

Preset's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Preset's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed
- Company policies are reviewed and signed by employees. Those same policies are posted in the Company intranet

Human Resource Policies and Practices

Preset's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensures the service organization is operating at maximum efficiency. Preset's human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement on their first day of employment
- Evaluations for each employee are performed on a semi-annual basis
- Employee termination procedures are in place to guide the termination process and are documented in Human Resource and Asset Management policies, as well as in a termination checklist

Security Management

Preset has a comprehensive security program in place that implements security current best practices in the industry.

The areas of focus include:

- Security Operations Center responsible for ongoing monitoring of attack surfaces
- Application and Infrastructure Security
- Endpoint Security
- Secure Software Development Lifecycle

- Business Continuity and Disaster Recovery
- Third Party Vendor Security
- Governance, Risk, and Compliance
- Physical Security
- Security Training
- Vulnerability Reporting Channel

The security roles are defined around each line of business to ensure that at least one entity is directly responsible for a particular control. All security roles regularly interact with the Director of Engineering, who serves as the acting Head of Security.

Security and Privacy Policies

Access Control Policy - To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy- To identify organizational assets and define appropriate protection responsibilities.

Business Continuity & Disaster Recovery Plan - To prepare Preset in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Cryptography Policy - To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.

Data Management Policy - To ensure that information is classified and protected in accordance with its importance to the organization.

Human Resources Policy - To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Incident Response Plan - Policy and procedures for suspected or confirmed information security incidents.

Mobile Device Security Policy - To secure Preset devices and devices that access Preset data.
Operations Security Policy- To ensure the correct and secure operation of information processing systems and facilities.

Password Policy - To establish standards for secure passwords.

Physical Security Policy - To prevent unauthorized physical access or damage to the organization's information and information processing facilities.

Privacy Policy - To define how Preset uses a users data and the rights of each party.

Risk Management Policy - To define the process for assessing and managing Preset's information security risks in order to achieve the company's business and information security objectives.

Secure Development Policy - To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Third-Party Management Policy - To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Personnel Security

We have robust personnel security procedures.

They include:

- Multi-stage hiring process
- Background Checks
- Recurring Security Training

- Company policy acceptance
- Anti-harassment Training
- Whistle-blower hotline
- Anonymous surveys

Physical Security and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

Change Management

Preset maintains documented Operational Security and Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Test results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Depending on the application, a software team peer or management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

System Monitoring

Preset uses a variety of platforms to perform system monitoring, including and not limited to the following:

- Vanta - Compliance automation
- Cloudwatch/Cloudtrail - Cloud infrastructure logging
- Datadog - Infrastructure and application monitoring
- WAF - Botnet, Georegion and DDOS monitoring
- Threat Stack - Container IDS monitoring
- Snyk - Vulnerability monitoring
- Sentry - Application monitoring
- Real User Monitoring (RUM) - Session monitoring
- JAMF - Endpoint monitoring

Incident Management

The Incident Response team follows an iterative response process designed to investigate, contain exploitation, remediate vulnerabilities, and document a post-mortem with the lessons of an incident.

Summary

- Incident declared
- Triage and analysis
- Investigation
- Containment & neutralization (short-term work)
- Hardening & detection improvements (lessons learned, long-term work)

System Account Management

Preset determines the type and level of access granted to individual users based on the “principle of least privilege.” This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by Preset business and security requirements. Permissions and access rights not expressly granted are, by default, prohibited.

Preset's primary method of assigning and maintaining consistent access controls and access rights is through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions are allocated to groups. Individual user accounts may be granted additional permissions as needed on an exception basis.

All access changes to the Production environment are handled via automated configuration management systems. This ensures that access control changes go through a formal code review process, and that they are automatically enforced and logged.

Administrators perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews are also documented.

Risk Management Program

Risk Management Responsibilities

CEO- Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.

VP of Engineering- Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register.

Director of Engineering, Data Protection Officer- Shall be responsible for the identification and treatment of all Information Security risks. This person shall be responsible for communicating risks to top management and adopting risk treatments in accordance with executive direction.

Integration with Risk Assessment

Preset evaluates the environment in which the system operates, which includes:

- the customer contractual commitments
- partner agreements
- regulatory compliance
- business responsibilities surrounding Preset's production system
- nature of the components of the system to determine which risks to assess.

Preset addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Preset's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Preset's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. At Preset, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Communication between employees occurs in the office, through remote meetings, Slack, Intranet, e-mails, and through other communication channels, to discuss operational efficiencies within employees' applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all-hands meetings are held periodically to provide staff with updates on the Company and key issues affecting the organization and its employees. Senior executives lead the all-hands meetings with information gathered from formal automated information systems and informal databases or spreadsheets, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Preset personnel via e-mail or other communication channels.

Specific information systems used to support Preset’s Data Analytics and Visualization Platform Services System are described in the Description of Services section above.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

All Security criteria were applicable to the Preset SaaS.

DC 9: Disclosures of Significant Changes In Last 1 Year

No changes have occurred within the last 12 months.